(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003年10月9日 (09.10.2003)

PCT

(10) 国際公開番号
WO 03/084125 A1

(51) 国際特許分類[7]: H04L 9/08, G11B 20/10, G06F 12/14, H04M 11/00

(21) 国際出願番号: PCT/JP03/02291

(22) 国際出願日: 2003年2月28日 (28.02.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-97429 2002年3月29日 (29.03.2002) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府 門真市 大字門真1006番地 Osaka (JP).

(72) 発明者; および

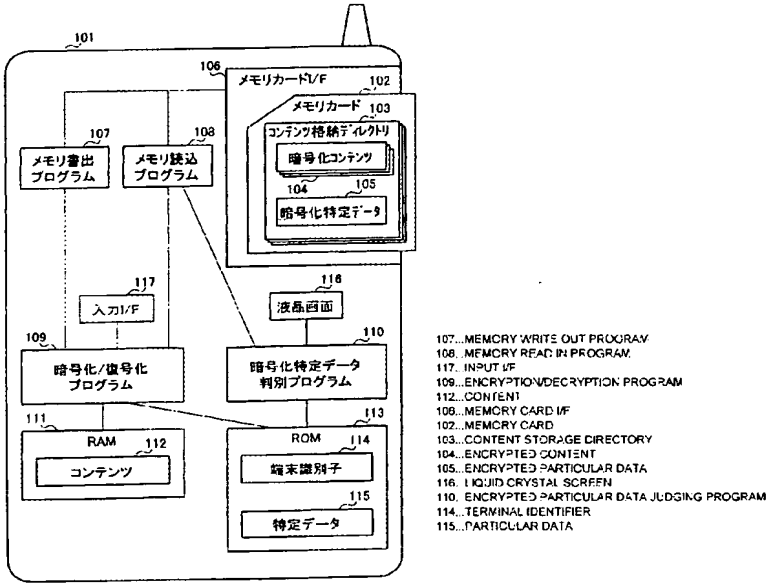
(75) 発明者/出願人 (米国についてのみ): 中井 信一 (NAKAI,Shinichi) [JP/JP]; 〒226-0024 神奈川県 横浜市 緑区西八朔町138-1-203 Kanagawa (JP). 野口 直彦 (NOGUCHI,Naohiko) [JP/JP]; 〒222-0031 神奈川県 横浜市 港北区太尾町1323-601 Kanagawa (JP). 松居 真一 (MATSUI,Shinichi) [JP/JP]; 〒658-0073 兵庫県 神戸市 東灘区西岡本1-5-16-302 Hyogo (JP). 難波 孝彰 (NANBA,Takaaki) [JP/JP]; 〒470-0115 愛知県 日進市 南ヶ丘2-4-13 Aichi (JP). 井上 隆司 (INOUE,Ryuji) [JP/JP]; 〒562-0005 大阪府 箕面市 新稲5-15-B-106 Osaka (JP).

(74) 代理人: 鷲田 公一 (WASHIDA,Kimihito); 〒206-0034 東京都 多摩市 鶴牧1丁目24-1 新都市センタービル 5階 Tokyo (JP).

[続葉有]

(54) Title: CONTENT PROCESSING DEVICE, CONTENT ACCUMULATION MEDIUM, CONTENT PROCESSING METHOD, AND CONTENT PROCESSING PROGRAM

(54) 発明の名称: コンテンツ処理装置、コンテンツ蓄積媒体、コンテンツ処理方法及びコンテンツ処理プログラム



(57) Abstract: For an encrypted content (104) stored in a content accumulation medium (102), small-data-amount information on the encrypted content (104) is stored in the content accumulation medium (102) in correlation to the encrypted content (104). Thus, without decrypting the large-data-amount encrypted content (104), it is possible to judge the encrypted content (104) according to the small-data-amount information. This enables a user to easily judge a plurality of contents stored in the content accumulation medium.

[続葉有]

WO 03/084125 A1

(81) 指定国 (国内): CN, JP, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR).

添付公開書類:
— 国際調査報告書

(57) 要約: コンテンツ蓄積媒体１０２に格納された暗号化コンテンツ１０４について、当該暗号化コンテンツ１０４に関連したデータ量の少ない情報を当該暗号化コンテンツ１０４に対応付けてコンテンツ蓄積媒体１０２に格納することにより、データ量の多い暗号化コンテンツ１０４を復号化することなく、関連した情報に基づいて暗号化コンテンツ１０４を判別することができる。これにより、コンテンツ蓄積媒体に格納された複数のコンテンツの判別を一段と容易に行うことができる。

明　細　書

コンテンツ処理装置、コンテンツ蓄積媒体、コンテンツ処理方法及びコンテンツ処理プログラム

技術分野

本発明は、コンテンツをコンテンツ蓄積媒体に格納して利用するための、コンテンツ処理装置、コンテンツ蓄積媒体、コンテンツ処理方法及びコンテンツ処理プログラムに関する。

背景技術

従来、携帯電話機等の端末装置において、コンテンツプロバイダから各種コンテンツをダウンロードし、これらのコンテンツを当該端末装置において利用するものがある。

コンテンツのダウンロードが可能である端末装置は、ダウンロードしたコンテンツを着脱自在の例えばメモリカードのようなコンテンツ蓄積媒体に格納することにより、内蔵メモリの容量を大きくすることなく、利用者に複数のコンテンツを提供することが可能となっている。これにより、端末装置の大型化を回避し、可搬性を確保することができる。

ところで、コンテンツ蓄積媒体にコンテンツを格納する場合、端末装置は当該コンテンツを所定の暗号化方法によって暗号化した後、これを格納するようになされている。これにより、コンテンツ蓄積媒体に格納されたコンテンツを他の利用環境において利用することを制限している。

また、コンテンツ蓄積媒体は、１つの端末装置だけではなく、複数の端末装置によって、暗号化されたコンテンツを格納することが可能となっている。これにより、利用者は、自分が所有する複数の端末装置においてダウンロードしたコンテンツを１つのメモリカードに格納することができる。

このように、１つのコンテンツ蓄積媒体には、異なる複数の端末装置によって格納されたコンテンツが混在する場合がある。コンテンツは、端末装置の種類やその構造によって使用可能な対象端末装置が異なっている。

従って、端末装置にコンテンツ蓄積媒体を装着し、当該コンテンツ蓄積媒体からコンテンツを読み出す場合、端末装置は、装着されたコンテンツ蓄積媒体からコンテンツを１つ１つ読み出し、各コンテンツを完全に復号化することによってはじめて当該コンテンツが利用可能であるか否かの判断を行うことが可能となっている。

このように、従来の端末装置においては、コンテンツ蓄積媒体に格納されている複数のコンテンツの中から、このとき使用する端末装置において利用可能であるコンテンツを見つけ出す作業として、装着されたコンテンツ蓄積媒体からすべてのコンテンツを１つ１つ読み出し、当該読み出されたコンテンツについて、順次、復号した後に利用可能であるか否かを判断するといった煩雑な作業が必要となり、当該作業にかかる時間が長くなるという問題があった。

また、従来の端末装置においては、コンテンツ蓄積媒体に格納されているコンテンツが使用可能であるか否かを判断することが困難な機種もある。このような場合、例えば、コンテンツとしてオーディオデータがコンテンツ蓄積媒体に格納されているとすると、このオーディオデータが端末装置にとって正規のデータでなくとも、その端末装置がこれを再生してしまう可能性があり、大音量が流れる等の不都合が生じる問題があった。

発明の開示

本発明の目的は、コンテンツ蓄積媒体に格納された複数のコンテンツの判別を一段と容易に行うことが可能なコンテンツ処理装置、コンテンツ蓄積媒体、コンテンツ処理方法及びコンテンツ処理プログラムを提供することである。

この目的は、コンテンツ蓄積媒体に格納された暗号化コンテンツについて、当該暗号化コンテンツに関連したデータ量の少ない情報を当該暗号化コンテ

ンツに対応付けてコンテンツ蓄積媒体に格納することにより、データ量の多い暗号化コンテンツを復号化することなく、関連した情報に基づいて暗号化コンテンツを判別することにより達成される。

5 図面の簡単な説明

図１は、本発明の実施の形態１に係るコンテンツ処理装置の構成を示す外観図、

図２は、実施の形態１に係るコンテンツ処理装置の構成を示すブロック図、

図３は、実施の形態１に係るコンテンツ処理装置のコンテンツ書出し処理手
10 順を示すフローチャート、

図４は、本発明の実施の形態１に係るコンテンツ蓄積媒体のデータ格納状態を示す略線図、

図５は、本発明の実施の形態１に係るコンテンツ処理装置のコンテンツ読込み処理手順を示すフローチャート、

15 図６は、実施の形態２に係るコンテンツ処理装置の構成を示すブロック図、

図７は、実施の形態２に係るコンテンツ処理装置のコンテンツ書出し処理手順を示すフローチャート、

図８は、本発明の実施の形態２に係るコンテンツ蓄積媒体のデータ格納状態を示す略線図、

20 図９は、本発明の実施の形態２に係るコンテンツ処理装置のコンテンツ読込み処理手順を示すフローチャート、

図１０は、実施の形態３に係るコンテンツ処理装置の構成を示すブロック図、

図１１は、実施の形態３に係るコンテンツ処理装置のコンテンツ書出し処理手順を示すフローチャート、

25 図１２は、本発明の実施の形態３に係るコンテンツ蓄積媒体のデータ格納状態を示す略線図、

図１３は、本発明の実施の形態３に係るコンテンツ処理装置のコンテンツ読

込み処理手順を示すフローチャート、

図１４は、実施の形態４に係るコンテンツ処理装置の構成を示すブロック図、

図１５は、実施の形態４に係るコンテンツ処理装置のコンテンツ書出し処理手順を示すフローチャート、

図１６は、本発明の実施の形態４に係るコンテンツ蓄積媒体のデータ格納状態を示す略線図、

図１７は、本発明の実施の形態４に係るコンテンツ処理装置のコンテンツ読込み処理手順を示すフローチャートは、

図１８は、実施の形態５に係るコンテンツ処理装置の構成を示すブロック図、

図１９は、実施の形態５に係るコンテンツ処理装置のコンテンツ書出し処理手順を示すフローチャート、

図２０は、本発明の実施の形態５に係るコンテンツ蓄積媒体のデータ格納状態を示す略線図、

図２１は、本発明の実施の形態５に係るコンテンツ処理装置のコンテンツ読込み処理手順を示すフローチャート、

図２２は、実施の形態６に係るコンテンツ処理装置の構成を示すブロック図、

図２３は、実施の形態６に係るコンテンツ処理装置のコンテンツ書出し処理手順を示すフローチャート、

図２４は、本発明の実施の形態６に係るコンテンツ蓄積媒体のデータ格納状態を示す略線図、

図２５は、本発明の実施の形態６に係るコンテンツ処理装置のコンテンツ読込み処理手順を示すフローチャート、

図２６は、実施の形態７に係るコンテンツ処理装置の構成を示すブロック図、

図２７は、実施の形態７に係るコンテンツ処理装置のコンテンツ書出し処理手順を示すフローチャート、

図２８は、本発明の実施の形態７に係るコンテンツ蓄積媒体のデータ格納状態を示す略線図、及び、

図２９は、本発明の実施の形態７に係るコンテンツ処理装置のコンテンツ読込み処理手順を示すフローチャートである。

発明を実施するための最良の形態

以下、本発明の実施の形態について、図面を参照して詳細に説明する。

（実施の形態１）

図１は、本発明の実施の形態１に係るコンテンツ処理装置としての携帯電話機１０１の外観を示す正面図である。

携帯電話機１０１は、携帯電話回線網を介して他の電話機器との間で通話を行う携帯電話機能部に加えて、コンテンツプロバイダから携帯電話回線網を介して音楽またはゲーム等の各種コンテンツをダウンロードするようになっている。

また、携帯電話機１０１は、コンテンツ蓄積媒体であるカード状の記憶媒体（メモリカード１０２）を着脱自在とするメモリカードインターフェイス（I/F）１０６を有し、当該メモリカードインターフェイス１０６に装着されたメモリカード１０２に対して、携帯電話機１０１の内部メモリに格納されているコンテンツなどの種々の情報を書き込む（以下、これを情報の書出しと称する）とともに、メモリカード１０２に格納されているコンテンツなどの種々の情報を読み出す（以下、これを情報の読込みと称する）ようになっている。

携帯電話機１０１の筐体正面部には、操作ボタン等からなる入力インターフェイス（I/F）１１７が設けられており、当該入力インターフェイス１１７を利用者が操作することにより、携帯電話機能を利用する際の電話番号等の入力に加えて、コンテンツのダウンロード、メモリカード１０２に対する各種情報の書き出し、読み込み等、種々のコマンドを入力することが可能となっている。

また、携帯電話機１０１の筐体正面部には、液晶表示部の液晶画面１１６が設けられており、携帯電話機１０１の動作に関する情報、コンテンツの実行に関する各種情報及びコンテンツの内容が表示される。

図１との対応部分に同一符号を付して示す図２は、携帯電話機１０１の構成を示すブロック図である。この図２は、携帯電話機１０１の構成のうち、特にコンテンツ処理に関わる構成を抽出して示すものである。携帯電話機１０１は、それぞれ図示しないＣＰＵ（Central Processing Unit）によって動作するメモリ書出プログラム１０７、メモリ読込プログラム１０８、暗号化/復号化プログラム１０９及び暗号化特定データ判別プログラム１１０を含んでいる。

図２において、携帯電話機１０１は、コンテンツプロバイダから携帯電話回線網を介してダウンロードしたコンテンツ１１２をＲＡＭ（Random Access Memory）１１１に格納する。暗号化/復号化プログラム１０９は、ＲＡＭ１１１に格納されたコンテンツ１１２を暗号化するものであり、当該暗号化/復号化プログラム１０９によって暗号化されたコンテンツ１１２は、暗号化コンテンツ１０４として、メモリ書出プログラム１０７によってメモリカードインターフェイス１０６を介してメモリカード１０２に書き込まれる。

ＲＯＭ（Read Only Memory）１１３は、携帯電話機１０１に固有の、例えば電話番号等でなる端末識別子１１４と、この実施の形態に示される、コンテンツをメモリカードに書き込みまたは読み出す処理を行うシステムに共通の、例えば文字列でなる特定データ１１５とを格納している。

暗号化/復号化プログラム１０９は、コンテンツ１１２を暗号化する際、ＲＯＭ（Read Only Memory）１１３に格納されている端末識別子１１４を用いて暗号化する。また、暗号化/復号化プログラム１０９は、コンテンツ１１２を暗号化してメモリカード１０２に格納する処理に伴って、ＲＯＭ１１３に格納されている特定データ１１５を端末識別子１１４で暗号化する。当該暗号化の結果である暗号化特定データ１０５は、メモリ書出プログラム１０７によってメモリカード１０２の暗号化コンテンツ１０４と同じディレクトリに格納される。このように、暗号化特定データ１０５を暗号化コンテンツ１０４と同じディレクトリに格納することにより、暗号化特定データ１０５と暗号化コンテンツとが対応付けられた状態でメモリカード１０２に格納される。

また、メモリカード１０２に格納された暗号化コンテンツ１０４を携帯電話機１０１に読み込む場合、携帯電話機１０１のメモリ読込プログラム１０８は、暗号化コンテンツ１０４を読み込む処理に先立って、当該暗号化コンテンツ１０４と同じディレクトリに格納されている暗号化特定データ１０５をメモリカード１０２からメモリカードインターフェイス１０６を介して読み込む。

当該読み込まれた暗号化特定データ１０５は、暗号化特定データ判別プログラム１１０によって復号化される。この場合、暗号化特定データ判別プログラム１１０は、ＲＯＭ１１３に格納されている携帯電話機１０１に固有の端末識別子１１４を用いて暗号化特定データを復号化するとともに、当該復号化された特定データとＲＯＭ１１３に格納されている特定データ１１５とを比較し、当該比較結果が一致した場合には、当該復号化したメモリカード１０２の暗号化特定データ１０５が、携帯電話機１０１によってメモリカード１０２に書き込まれたものであると判別することができる。

このように、メモリカード１０２に格納されている暗号化特定データ１０５が、携帯電話機１０１によってメモリカード１０２に書き込まれたものであることが判ると、暗号化/復号化プログラム１０９は、当該暗号化特定データ１０５と同じディレクトリに格納されている暗号化コンテンツ１０４を復号化し、当該復号化されたコンテンツ１１２をＲＡＭ１１１に格納する。

図３は、携帯電話機１０１のＲＡＭ１１１に格納されているコンテンツ１１２を、メモリカード１０２に格納する際の、暗号化/復号化プログラム１０９の処理手順を示すフロー図である。

図３に示すように、暗号化/復号化プログラム１０９は、ステップＳＴ２０１において、ＲＯＭ１１３から特定データ１１５及び端末識別子１１４を取得する。そして、暗号化/復号化プログラム１０９は、ステップＳＴ２０２に移って、ステップＳＴ２０１において取得した特定データ１１５を、ステップＳＴ２０１において取得した携帯電話機１０１に固有の端末識別子１１４を用いて、例えばトリプルＤＥＳ（Data Encryption Standard）暗号方式によって暗号化す

ることにより、暗号化特定データ１０５を生成する。

そして、暗号化/復号化プログラム１０９は、ステップＳＴ２０３に移って、このときメモリカードインターフェイス１０６に装着されているメモリカード１０２に、ステップＳＴ２０２において生成された暗号化特定データ１０５と同じ暗号化特定データが既に格納されているか否かを判断する。ここで否定結果が得られると、このことは、メモリカード１０２には、携帯電話機１０１に固有の端末識別子１１４を用いて暗号化された暗号化特定データ１０５、すなわち、携帯電話機１０１によって書き出された暗号化特定データ１０５が格納されていないことを意味しており、このとき暗号化/復号化プログラム１０９は、ステップＳＴ２０４に移って、ステップＳＴ２０２において暗号化された暗号化特定データ１０５を、メモリ書出プログラム１０７を用いてメモリカード１０２に格納した後、ステップＳＴ２０５に移る。

また、ステップＳＴ２０３において肯定結果が得られると、このことは、メモリカード１０２には、携帯電話機１０１によって書き出された暗号化特定データ１０５が格納されていることを意味しており、このとき暗号化/復号化プログラム１０９は、ステップＳＴ２０５に移る。

ステップＳＴ２０５において、暗号化/復号化プログラム１０９は、ＲＡＭ１１１からコンテンツ１１２を取得した後、ステップＳＴ２０６に移って、ステップＳＴ２０５において取得したコンテンツ１１２を、ＲＯＭ１１３内の端末識別子１１４を用いて例えばトリプルＤＥＳ暗号方式で暗号化する。

そして、暗号化/復号化プログラム１０９は、ステップＳＴ２０７に移って、ステップＳＴ２０６において暗号化された暗号化コンテンツ１０４を、ステップＳＴ２０４においてメモリカード１０２に格納された暗号化特定データ１０５と同じディレクトリに格納する。

これにより、図４に示すように、メモリカード１０２においては、それぞれ同じ端末識別子１１４によって暗号化されたコンテンツ１１２（暗号化コンテンツ１０４）と特定データ１１５（暗号化特定データ１０５）とが、同じディ

レクトリ３０１、３０２に格納された状態となる。このように、暗号化コンテンツ１０４と暗号化特定データ１０５とを同じディレクトリに格納することにより、これらのデータは対応付けられてメモリカード１０２に格納された状態となる。

また、図５は、図３の処理手順によってメモリカード１０２に格納された暗号化コンテンツ１０４と暗号化特定データとを携帯電話機１０１によって読み込んで復号化する際の、暗号化/復号化プログラム１０９と暗号化特定データ判別プログラム１１０との処理手順を示すフロー図である。

図５に示すように、暗号化特定データ判別プログラム１１０は、ステップＳＴ４０１において、メモリカード１０２内に暗号化特定データ１０５があるか否かを調べる。ここで否定結果が得られると、このことは、メモリカード１０２には、読み込むべき暗号化特定データ１０５がないこと、すなわち、当該暗号化特定データ１０５に対応付けられた暗号化コンテンツ１０４がないことを意味しており、このとき暗号化特定データ判別プログラム１１０は、この処理手順を終了する。

これに対して、ステップＳＴ４０１において肯定結果が得られると、このことは、メモリカード１０２には、読み込むべき暗号化特定データ１０５があること、すなわち、当該暗号化特定データ１０５に対応付けられた暗号化コンテンツ１０４があることを意味しており、このとき暗号化特定データ判別プログラム１１０は、ステップＳＴ４０２に移って、メモリ読込プログラム１０８を用いてメモリカード１０２から暗号化特定データ１０５を取得した後、ステップＳＴ４０３に移る。ステップＳＴ４０３において、暗号化特定データ判別プログラム１１０は、ステップＳＴ４０２において取得した暗号化特定データ１０５を、ＲＯＭ１１３に格納されている端末識別子１１４を用いて復号化する。

そして、暗号化特定データ判別プログラム１１０は、ステップＳＴ４０４に移って、ステップＳＴ４０３において復号化された特定データと、ＲＯＭ１１３に格納されている特定データ１１５とを比較し、復号化された特定データと、

ＲＯＭ１１３に格納されている特定データ１１５とが同一であるか否かを判断する。

因みに、携帯電話機１０１は、コンテンツ１１２を暗号化してメモリカード１０２に書き出す場合には、常に、特定データ１１５を端末識別子１１４を用いて暗号化することにより得られる暗号化特定データ１０５を、暗号化コンテンツ１０４に対応付けて格納するようになっている。従って、ステップＳＴ４０３において復号化された特定データと、ＲＯＭ１１３に格納されている特定データ１１５との比較結果が一致する場合、このことは、このとき復号化された暗号化特定データ１０５がその携帯電話機１０１によってメモリカード１０２に書き出されたもの、すなわち、当該暗号化特定データ１０５と対応付けられてメモリカード１０２に格納されている暗号化コンテンツ１０４が携帯電話機１０１によってメモリカード１０２に書き出されたものであることを意味する。

従って、ステップＳＴ４０３において復号化された特定データと、ＲＯＭ１１３に格納されている特定データ１１５との比較結果が一致する場合、暗号化特定データ判別プログラム１１０は、当該一致結果を暗号化/復号化プログラム１０９に通知するとともに、ステップＳＴ４０４からテップＳＴ４０５に移る。

これに対して、ステップＳＴ４０３において復号化された特定データと、ＲＯＭ１１３に格納されている特定データ１１５との比較結果が一致しない場合、暗号化特定データ判別プログラム１１０は、当該不一致の結果を暗号化/復号化プログラム１０９に通知するとともに、上述のステップＳＴ４０１に戻って、メモリカード１０２内に次の暗号化特定データがあるか否かを判断し、次の暗号化特定データがある場合には、その暗号化特定データについて同様の処理を実行する。

ステップＳＴ４０５において、暗号化特定データ判別プログラム１１０は、上述のステップＳＴ４０４において一致結果が得られた暗号化特定データ１０５及び当該暗号化特定データ１０５が格納されているディレクトリ３０２

に格納されているすべての暗号化特定データを暗号化/復号化プログラム１０９に復号化させ、その一覧を液晶画面１１６に表示する。

これにより、液晶画面１１６には、メモリカード１０２に格納されている暗号化コンテンツのうち、携帯電話機１０１によって利用可能な暗号化コンテンツ１０４に対応付けられた特定データ１１５の一覧が表示される。すなわち、携帯電話機１０１によって利用可能な暗号化コンテンツ１０４が、それに対応付けられたデータ量の少ない特定データ１１５によって一覧表示される。

因みに、この実施の形態においては、暗号化コンテンツ１０４に対応付けられた暗号化特定データ１０５を復号化して一覧表示する場合について述べたが、これに限らず、暗号化コンテンツ１０４を特定データ１１５に対応付けてメモリカード１０２に格納する際に、その特定データ１１５に対応したコンテンツのタイトルのみを携帯電話機１０１のＲＡＭ１１１に格納し、ステップＳＴ４０４における特定データ１０５の一致結果に基づいて、当該格納されているタイトルを一覧表示するようにしてもよい。

ステップＳＴ４０５において、液晶画面１１６にコンテンツの一覧が表示されると、利用者は、入力インターフェイス１１７を操作することにより、当該表示された一覧のなかから所望とするコンテンツを選択する。

これにより、暗号化/復号化プログラム１０９は、ステップＳＴ４０６に移って、メモリ読込プログラム１０８を用いて、このとき入力インターフェイス１１７を介して指定された暗号化コンテンツ１０４をメモリカード１０２から読み込み、さらに続くステップＳＴ４０７に移って、ステップＳＴ４０６においてメモリカード１０２から取得した暗号化コンテンツ１０４を、ＲＯＭ１１３に格納されている端末識別子１１４を用いて復号化し、ＲＡＭ１１１に格納する。

ＲＡＭ１１１に格納されたコンテンツ１１１は、携帯電話機１０１の利用者が入力インターフェイス１１７を操作することにより起動され、利用者の利用に供される。

以上の構成において、携帯電話機１０１は、メモリカード１０２に暗号化コンテンツ１０４を書き出す際に、当該暗号化コンテンツ１０４に対応付けられた暗号化特定データ１０５をメモリカード１０２に格納しておく。

この暗号化特定データ１０５は、例えば、ある文字列を暗号化したものであり、暗号化コンテンツ１０４に比べてそのデータ量は格段に少ないものとなっている。従って、携帯電話機１０１は、メモリカード１０２から暗号化コンテンツ１０４を読み込んで復号化する前に、当該暗号化コンテンツ１０４に対応付けられた暗号化特定データ１０５を読み込んでこれを復号化し、当該復号化された特定データが携帯電話機１０１によってメモリカード１０２に書き出されたものであるか否かを判別する。

復号化された特定データが携帯電話機１０１によってメモリカード１０２に書き出されたものである場合、当該特定データに対応付けられてメモリカード１０２に格納されている暗号化コンテンツ１０４も携帯電話機１０１によってメモリカード１０２に書き出されたものであることになる。

従って、この場合、メモリカード１０２に格納されている暗号化コンテンツ１０４は、携帯電話機１０１に読み込んで、当該携帯電話機１０１によって利用することが可能であり、携帯電話機１０１の暗号化/復号化プログラム１０９は、メモリカード１０２から暗号化コンテンツ１０４を読み込み、当該読み込まれた暗号化コンテンツ１０４を復号化する。

このように、暗号化特定データ１０５の復号結果が、ＲＯＭ１１３に格納されている特定データ１１５と一致することを条件に、当該暗号化特定データ１０５に対応付けられた暗号化コンテンツ１０４をメモリカード１０２から携帯電話機１０１に読み込んで復号化することにより、携帯電話機１０１は、当該携帯電話機１０１において利用可能である暗号化コンテンツ１０４のみを選択的に復号化することができる。

従って、メモリカード１０２に複数の暗号化コンテンツが格納されている状態であって、これら複数の暗号化コンテンツを利用可能な端末装置（携帯電話

機等）が各暗号化コンテンツ毎に異なる場合であっても、携帯電話機１０１は、これら複数のデータ量の多い暗号化コンテンツをすべて復号化する必要はなく、当該複数の暗号化コンテンツにそれぞれ対応付けられた、データ量の少ない暗号化特定データを復号化するだけで、利用可能な暗号化コンテンツ１０４を判別することができる。

このように、本実施の形態のコンテンツ処理装置としての携帯電話機１０１によれば、コンテンツ蓄積媒体であるメモリカード１０２に格納された複数の暗号化コンテンツの判別を一段と容易に行うことが可能となり、携帯電話機１０１において利用可能な暗号化コンテンツ１０４を一段と迅速に復号化することができる。

なお、この実施の形態の携帯電話機１０１においては、端末識別子１１４として、その携帯電話機１０１の電話番号を用いる場合について述べたが、これに限らず、例えば携帯電話機１０１の製造番号のようなその携帯電話機１０１を識別するための識別子、又は、その他の何らかの意味を持つ文字列、数値、画像または音声等のデータ、若しくは特定のサービスと契約したことを示す識別子（会員番号等）を用いるようにしてもよい。また、この端末識別子１１４として電話番号、製造番号、又はその他の文字列等の情報そのものではなく、端末識別子に対してある変換を加えた結果（端末識別子に関連する情報）を用いるようにしてもよい。このようにすれば、端末識別子によってコンテンツ及び特定データを暗号化する際の暗号化方法、及び端末識別子が第三者に漏洩した場合であっても、その端末識別子は、暗号化鍵となり得る他のデータに変換されていることにより、このデータ（暗号化鍵）によって暗号化された暗号化コンテンツ及び暗号化特定データが解読されることを防止することができる。

また、この実施の形態の携帯電話機１０１においては、特定データ１１５として、コンテンツをメモリカードに書き込みまたは読み出す処理を行うシステムに共通の、例えば文字列を用いる場合について述べたが、これに限らず、端末識別子として設定されている情報とは異なる他の識別子（例えば端末識別子

１１４として電話番号が設定されている場合は、特定データとして製造番号）、その他の何らかの意味を持つ文字列、数値、画像または音声等のデータ、若しくは特定のサービスと契約したことを示す識別子（会員番号等）を用いるようにしてもよい。

また、この実施の形態においては、コンテンツを格納するコンテンツ蓄積媒体としてメモリカード１０２を用いる場合について述べたが、これに限らず、要はデジタル情報化されたコンテンツを格納可能なコンテンツ蓄積媒体であれば、他のデバイスを広く適用することができる。

（実施の形態２）

図６は、本発明の実施の形態２に係るコンテンツ処理装置としての携帯電話機５０１の構成を示すブロック図である。但し、図１及び図２と同一の構成となるものについては、図１及び図２と同一番号を付し、詳しい説明を省略する。

この図６に示される携帯電話機５０１は、認証プログラム５１０を有し、当該認証プログラム５１０によって認証を行うことによりアクセスが可能となる認証領域５０４をメモリカード５０２に設け、当該認証領域５０４に暗号化特定データ５０４を格納するようにした点が図２の構成の携帯電話機１０１と異なる。

図２との対応部分に同一符号を付して示す図６は、携帯電話機５０１の構成を示すブロック図である。この図６は、携帯電話機５０１の構成のうち、特にコンテンツ処理に関わる構成を抽出して示すものである。携帯電話機５０１は、それぞれ図示しないＣＰＵ（Central Processing Unit）によって動作するメモリ書出プログラム１０７、メモリ読込プログラム１０８、暗号化/復号化プログラム５１３、暗号化特定データ判別プログラム５１４及び認証プログラム５１０を含んでいる。

図６において、携帯電話機５０１は、コンテンツプロバイダから携帯電話回線網を介してダウンロードしたコンテンツ５１６をＲＡＭ（Random Access Memory）５１５に格納する。暗号化/復号化プログラム５１３は、ＲＡＭ５１

５に格納されたコンテンツ５１６を暗号化するものであり、当該暗号化/復号化プログラム５１３によって暗号化されたコンテンツ５１６は、暗号化コンテンツ５０７として、メモリ書出プログラム１０７によってメモリカードインターフェイス１０６を介してメモリカード５０２の通常領域５０５に書き込まれる。通常領域５０５は、携帯電話機５０１に設けられた認証プログラム５１０の認証を必要とせずにアクセス可能な領域である。

ＲＯＭ（Read Only Memory）５１７は、携帯電話機５０１に固有の、例えば電話番号等でなる端末識別子５１８と、この実施の形態に示されるコンテンツをメモリカードに書き込み、または読み出す処理を行うシステムに共通の、例えば文字列でなる特定データ５１９とを格納している。

暗号化/復号化プログラム５１３は、コンテンツ５１６を暗号化する際、ＲＯＭ（Read Only Memory）５１７に格納されている端末識別子５１８を用いて暗号化する。また、暗号化/復号化プログラム５１３は、コンテンツ５１６を暗号化してメモリカード５０２に格納する処理に伴って、ＲＯＭ５１７に格納されている特定データ５１９を端末識別子５１８で暗号化する。当該暗号化の結果である暗号化特定データ５０４は、メモリ書出プログラム１０７によってメモリカード５０２の認証領域５０３に格納される。この認証領域５０３における暗号化特定データ５０４は、通常領域５０５の暗号化コンテンツ５０７が格納されるディレクトリと同じディレクトリに格納されるリンク情報５０８によって暗号化コンテンツ５０７と対応付けられる。このように、暗号化特定データ５０４及び暗号化コンテンツ５０７は、リンク情報５０８によって対応付けられて、認証領域５０３及び通常領域５０５に分けて格納される。

また、メモリカード５０２に格納された暗号化コンテンツ５０７を携帯電話機５０１に読み込む場合、携帯電話機５０１のメモリ読込プログラム１０８は、暗号化コンテンツ５０７を読み込む処理に先立って、当該暗号化コンテンツ５０７と同じディレクトリに格納されているリンク情報５０８によって対応付けられた、認証領域５０３の暗号化特定データ５０４をメモリカード５０２か

らメモリカードインターフェイス１０６を介して読み込む。

当該読み込まれた暗号化特定データ５０４は、暗号化特定データ判別プログラム５１４によって復号化される。この場合、暗号化特定データ判別プログラム５１４は、ＲＯＭ５１７に格納されている携帯電話機５０１に固有の端末識別子５１８を用いて暗号化特定データ５０４を復号化することにより、当該復号化された特定データとＲＯＭ５１７に格納されている特定データ５１９とが一致した場合には、当該復号化したメモリカード５０２の暗号化特定データ５０４が、携帯電話機５０１によってメモリカード５０２に書き込まれたものであると判別することができる。

このように、メモリカード５０２に格納されている暗号化特定データ５０４が、携帯電話機５０１によってメモリカード５０２に書き込まれたものであることが判ると、暗号化/復号化プログラム５１３は、当該暗号化特定データ５０４に対応付けられた、通常領域５０５の暗号化コンテンツ５０７を復号化し、当該復号化されたコンテンツ５１６をＲＡＭ５１５に格納する。

図７は、携帯電話機５０１のＲＡＭ５１６に格納されているコンテンツ５１６を、メモリカード５０２に格納する際の、認証プログラム５１０及び暗号化/復号化プログラム５１３の処理手順を示すフロー図である。

図７に示すように、認証プログラム５１０は、ステップＳＴ６０１において、まず、メモリカード５０２との間で認証を行う。因みに、メモリカード５０２には、図示しない認証プログラムが設けられており、携帯電話機５０１の認証プログラム５１０との間で認証処理を行い、当該認証結果として携帯電話機５０１がメモリカード５０２の認証領域５０３にアクセス可能である端末装置であるという結果が得られると、認証領域５０３へのアクセスを許可するようになされている。

ステップＳＴ６０１における認証処理の結果として、携帯電話機５０１からメモリカード５０２の認証領域５０３へのアクセスが可能になると、認証プログラム５１０は、当該認証結果を暗号化/復号化プログラム５１３に通知する。

この通知を受け取った暗号化/復号化プログラム５１３は、ステップＳＴ６０２において、ＲＯＭ５１７から特定データ５１９を取得する。そして、暗号化/復号化プログラム５１３は、ステップＳＴ６０３に移って、ステップＳＴ６０２において取得した特定データ５１９を、ＲＯＭ５１７に格納されている、携帯電話機５０１に固有の端末識別子５１８を用いて、例えばトリプルＤＥＳ暗号方式によって暗号化することにより、暗号化特定データ５０４を生成する。

そして、暗号化/復号化プログラム５１３は、ステップＳＴ６０４に移って、このときメモリカードインターフェイス１０６に装着されているメモリカード５０２の認証領域５０３に、ステップＳＴ６０３において生成された暗号化特定データ５０４と同じ暗号化特定データが既に格納されているか否かを判断する。ここで否定結果が得られると、このことは、メモリカード５０２には、携帯電話機５０１に固有の端末識別子５１８を用いて暗号化された暗号化特定データ５０４、すなわち、携帯電話機５０１によって書き出された暗号化特定データ５０４が格納されていないことを意味しており、このとき暗号化/復号化プログラム５１３は、ステップＳＴ６０５に移って、ステップＳＴ６０３において暗号化された暗号化特定データ５０４とリンク情報５０８を、メモリ書出プログラム１０７を用いてメモリカード５０２に格納した後、ステップＳＴ６０６に移る。この場合、暗号化/復号化プログラム５１３は、暗号化特定データ５０４を認証領域５０３に格納するとともに、リンク情報５０８を通常領域５０５のコンテンツ格納ディレクトリ５０６に格納する。リンク情報５０８は、認証領域５０３に格納された暗号化特定データ５０４と、これに対応付けられた、通常領域５０５の暗号化コンテンツ５０７とを対応付けるための情報である。

また、ステップＳＴ６０４において肯定結果が得られると、このことは、メモリカード５０２には、携帯電話機５０１によって書き出された暗号化特定データ５０４が格納されていることを意味しており、このとき暗号化/復号化プログラム５１３は、ステップＳＴ６０６に移る。

ステップＳＴ６０６において、暗号化/復号化プログラム５１３は、ＲＡＭ５１５からコンテンツ５１６を取得した後、ステップＳＴ６０７に移って、ステップＳＴ６０６において取得したコンテンツ５１６を、ＲＯＭ５１７内の端末識別子５１８を用いて例えばトリプルＤＥＳ暗号方式で暗号化する。

そして、暗号化/復号化プログラム５１３は、ステップＳＴ６０８に移って、ステップＳＴ６０７において暗号化された暗号化コンテンツ５０７を、ステップＳＴ６０５においてメモリカード５０２に格納された暗号化特定データ５０４とリンク情報５０８によって対応付けられたディレクトリに格納する。

これにより、図８に示すように、メモリカード５０２においては、それぞれ同じ端末識別子５１８によって暗号化されたコンテンツ５１６（暗号化コンテンツ５０７）と特定データ５１９（暗号化特定データ５０４）とが、リンク情報５０８によって対応付けられて格納された状態となる。このように、暗号化コンテンツ５０７と暗号化特定データ５０４とをリンク情報５０８によって対応付けるとともに、暗号化コンテンツ５０７の存在を確認するための暗号化特定データ５０４を認証領域５０３に格納することにより、認証領域５０３にアクセスが可能な携帯電話機５０１のみによって暗号化コンテンツ５０７の存在を確認することが可能な状態となる。

また、図９は、図７の処理手順によってメモリカード５０２に格納された暗号化コンテンツ５０７と暗号化特定データ５０４とを携帯電話機５０１によって読み込んで復号化する際の、暗号化/復号化プログラム５１３と暗号化特定データ判別プログラム５１４との処理手順を示すフロー図である。

図９に示すように、暗号化特定データ判別プログラム５１４は、ステップＳＴ７０１において、メモリカード５０２の通常領域５０５にリンク情報５０８があるか否かを判断する。ここで否定結果が得られると、このことは、リンク情報５０８がメモリカード５０２に格納されていないこと、すなわち、暗号化コンテンツ５０７が格納されていないことを意味しており、このとき暗号化特定データ判別プログラム５１４は、当該処理手順を終了する。

これに対して、ステップＳＴ７０１において肯定結果が得られると、このことは、リンク情報５０８がメモリカード５０２に格納されていること、すなわち、暗号化コンテンツ５０７が存在することを意味しており、このとき、暗号化特定データ判別プログラム５１４は、ステップＳＴ７０２に移って、認証プログラム５１０による認証処理を行った上で、メモリ読込プログラム１０８を用いてメモリカード５０２から、リンク情報５０８に対応する暗号化特定データ５０４を認証領域５０３から取得する。

そして、暗号化特定データ判別プログラム５１４は、ステップＳＴ７０３に移って、ステップＳＴ７０２において取得した暗号化特定データ５０４を、ＲＯＭ５１７に格納されている端末識別子５１８を用いて復号化する。

そして、暗号化特定データ判別プログラム５１４は、ステップＳＴ７０４に移って、ステップＳＴ７０３において復号化された特定データと、ＲＯＭ５１７に格納されている特定データ５１９とを比較し、復号化された特定データと、ＲＯＭ５１７に格納されている特定データ５１９とが同一であるか否かを判断する。

因みに、携帯電話機５０１は、コンテンツ５１６を暗号化してメモリカード５０２に書き出す場合には、常に、特定データ５１９を端末識別子５１８を用いて暗号化することにより得られる暗号化特定データ５０４を、暗号化コンテンツ５０７に対応付けて格納するようになっている。従って、ステップＳＴ７０３において復号化された特定データと、ＲＯＭ５１７に格納されている特定データ５１９との比較結果が一致する場合、このことは、このとき復号化された暗号化特定データ５０４が携帯電話機５０１によってメモリカード５０２に書き出されたもの、すなわち、当該暗号化特定データ５０４とリンク情報５０８によって対応付けられてメモリカード５０２に格納されている暗号化コンテンツ５０７が携帯電話機５０１によってメモリカード５０２に書き出されたものであることを意味する。

従って、ステップＳＴ７０３において復号化された特定データと、ＲＯＭ５

１７に格納されている特定データ５１９との比較結果が一致する場合、暗号化特定データ判別プログラム５１４は、当該一致結果を暗号化/復号化プログラム５１３に通知するとともに、ステップＳＴ７０４からテップＳＴ７０５に移る。

これに対して、ステップＳＴ７０３において復号化された特定データと、ＲＯＭ５１７に格納されている特定データ５１９との比較結果が一致しない場合、暗号化特定データ判別プログラム５１４は、当該不一致の結果を暗号化/復号化プログラム５１３に通知するとともに、上述のステップＳＴ７０１に戻って、メモリカード５０２内に次のリンク情報５０８があるか否かを判断し、次のリンク情報５０８がある場合には、そのリンク情報５０８について同様の処理を実行する。

ステップＳＴ７０５において、暗号化特定データ判別プログラム５１４は、上述のステップＳＴ７０４において一致結果が得られた特定データ５１９の一覧を液晶画面１１６に表示する。すなわち、携帯電話機５０１によって利用可能な暗号化コンテンツ５０７が、それに対応付けられたデータ量の少ない特定データ５１９によって一覧表示される。

因みに、この実施の形態においては、暗号化コンテンツ５０７に対応付けられた暗号化特定データ５０４を復号化して一覧表示する場合について述べたが、これに限らず、暗号化コンテンツ５０７を特定データ５１６に対応付けてメモリカード５０２に格納する際に、その特定データ５１６に対応したコンテンツのタイトルのみを携帯電話機５０１のＲＡＭ５１５に格納し、ステップＳＴ７０４における特定データ５１９の一致結果に基づいて、当該格納されているタイトルを一覧表示するようにしてもよい。

ステップＳＴ７０５において、液晶画面１１６にコンテンツの一覧が表示されると、利用者は、入力インターフェイス１１７を操作することにより、当該表示された一覧のなかから所望とするコンテンツを選択する。

これにより、暗号化/復号化プログラム５１３は、ステップＳＴ７０６に移って、メモリ読込プログラム１０８を用いて、このとき入力インターフェイス１

１７を介して指定された暗号化コンテンツ５０７をメモリカード５０２から読み込み、さらに続くステップＳＴ７０７に移って、ステップＳＴ７０６においてメモリカード５０２から取得した暗号化コンテンツ５０７を、ＲＯＭ５１７に格納されている端末識別子５１８を用いて復号化し、ＲＡＭ５１５に格納する。

ＲＡＭ５１５に格納されたコンテンツ５１６は、携帯電話機５０１の利用者が入力インターフェイス１１７を操作することにより起動され、利用者の利用に供される。

以上の構成において、携帯電話機５０１は、メモリカード５０２に暗号化コンテンツ５０７を書き出す際に、当該暗号化コンテンツ５０７に対応付けられた暗号化特定データ５０４をメモリカード５０２の認証領域５０３に格納しておく。

この暗号化特定データ５０４は、例えば、ある文字列を暗号化したものであり、暗号化コンテンツ５０７に比べてそのデータ量は格段に少ないものとなっている。従って、携帯電話機５０１は、メモリカード５０２から暗号化コンテンツ５０７を読み込んで復号化する前に、当該暗号化コンテンツ５０７に対応付けられた暗号化特定データ５０４を読み込んでこれを復号化し、当該復号化された特定データが携帯電話機５０１によってメモリカード５０２に書き出されたものであるか否かを判別することにより、データ量の少ない特定データに基づいて、携帯電話機５０１において利用可能なコンテンツがメモリカード５０２に存在するか否かを容易に判断することができる。

この実施の形態の場合、暗号化特定データ５０４は、認証領域５０３に格納されていることにより、携帯電話機５０１からメモリカード５０２の認証領域５０３へのアクセスは、認証処理を行った上で実行される。従って、認証領域５０３へのアクセスが可能な携帯電話機５０１以外の端末装置では、暗号化特定データ５０４の取得が困難となることにより、利用可能である暗号化コンテンツの判別を容易に行うことは困難となる。

このように、本実施の形態のコンテンツ処理装置としての携帯電話機５０１によれば、コンテンツ蓄積媒体であるメモリカード５０２に格納された複数の暗号化コンテンツの判別を、認証が可能な携帯電話機５０１においてのみ一段と容易に行うことが可能となる。

なお、この実施の形態の携帯電話機５０１においては、端末識別子５１８として、その携帯電話機５０１の電話番号を用いる場合について述べたが、これに限らず、例えば携帯電話機５０１の製造番号のようなその携帯電話機５０１を識別するための識別子、又は、その他の何らかの意味を持つ文字列、数値、画像または音声等のデータ、若しくは特定のサービスと契約したことを示す識別子（会員番号等）を用いるようにしてもよい。また、この端末識別子５１８として電話番号、製造番号、又はその他の文字列等の情報そのものではなく、端末識別子に対してある変換を加えた結果（端末識別子に関連する情報）を用いるようにしてもよい。このようにすれば、端末識別子によってコンテンツ及び特定データを暗号化する際の暗号化方法、及び端末識別子が第三者に漏洩した場合であっても、その端末識別子は、暗号化鍵となり得る他のデータに変換されていることにより、このデータ（暗号化鍵）によって暗号化された暗号化コンテンツ及び暗号化特定データが解読されることを防止することができる。

また、この実施の形態の携帯電話機５０１においては、特定データ５１９として、コンテンツをメモリカードに書き込みまたは読み出す処理を行うシステムに共通の、例えば文字列を用いる場合について述べたが、これに限らず、端末識別子として設定されている情報とは異なる他の識別子（例えば端末識別子５１８として電話番号が設定されている場合は、特定データとして製造番号）、その他の何らかの意味を持つ文字列、数値、画像または音声等のデータ、若しくは特定のサービスと契約したことを示す識別子（会員番号等）を用いるようにしてもよい。

また、この実施の形態においては、通常領域に格納されたリンク情報によって認証領域の暗号化特定データを特定する場合について述べたが、これに限ら

ず、例えば、通常領域に格納されている暗号化コンテンツの当該通常領域での格納位置を示す情報（ルート名、ディレクトリ名等）と、これに対応して認証領域に格納されている暗号化特定データの当該認証領域での格納位置を示す情報（ルート名、ディレクトリ名等）を同一とするようにしてもよい。このように同じディレクトリ構成とすれば、リンク情報を用いることなく認証領域での暗号化特定データと通常領域の暗号化コンテンツとを対応付けることができる。

また、この実施の形態においては、コンテンツを格納するコンテンツ蓄積媒体としてメモリカード５０２を用いる場合について述べたが、これに限らず、要はデジタル情報化されたコンテンツを格納可能なコンテンツ蓄積媒体であれば、他のデバイスを広く適用することができる。

（実施の形態３）

図１０は、本発明の実施の形態３に係るコンテンツ処理装置としての携帯電話機９０１の構成を示すブロック図である。但し、図１及び図２と同一の構成となるものについては、図１及び図２と同一番号を付し、詳しい説明を省略する。

この図１０に示される携帯電話機９０１は、ＲＯＭ９１３に格納される端末識別子９１４として、メモリカード９０２における暗号化コンテンツ９０５を格納するディレクトリ名とし、当該ディレクトリ名を特定データ１１５（図２）の代わりとして用いるようにした点が図２の構成の携帯電話機１０１と異なる。

図２との対応部分に同一符号を付して示す図１０は、携帯電話機９０１の構成を示すブロック図である。この図１０は、携帯電話機９０１の構成のうち、特にコンテンツ処理に関わる構成を抽出して示すものである。携帯電話機９０１は、それぞれ図示しないＣＰＵ（Central Processing Unit）によって動作するメモリ書出プログラム１０７、メモリ読込プログラム１０８、暗号化/復号化プログラム９０９及びコンテンツ格納ディレクトリ判別プログラム９１０を

含んでいる。

図１０において、携帯電話機９０１は、コンテンツプロバイダから携帯電話回線網を介してダウンロードしたコンテンツ９１２をＲＡＭ（Random Access Memory）９１１に格納する。暗号化/復号化プログラム９０９は、ＲＡＭ９１１に格納されたコンテンツ９１２を暗号化するものであり、当該暗号化/復号化プログラム９０９によって暗号化されたコンテンツ９１２は、暗号化コンテンツ９０５として、メモリ書出プログラム１０７によってメモリカードインターフェイス１０６を介してメモリカード９０２に書き込まれる。

ＲＯＭ（Read Only Memory）９１３は、携帯電話機９０１に固有の所定の文字列でなる識別子であって、暗号化コンテンツをメモリカード９０２に格納する際に用いられるディレクトリ名９０４となる端末識別子９１４を格納している。

暗号化/復号化プログラム９０９は、コンテンツ９１２を暗号化する際、ＲＯＭ（Read Only Memory）９１３に格納されている端末識別子９１４を用いて暗号化する。また、暗号化/復号化プログラム９０９は、当該暗号化されたコンテンツ９１２（暗号化コンテンツ９０５）をメモリカード９０２に格納する際、当該格納先となるコンテンツ格納ディレクトリ（以下、これを単にディレクトリと称する）９０３のディレクトリ名９０４を、ＲＯＭ９１３に格納されている端末識別子９１４とする。

また、メモリカード９０２に格納された暗号化コンテンツ９０５を携帯電話機９０１に読み込む場合、携帯電話機９０１のメモリ読込プログラム１０８は、暗号化コンテンツ９０５を読み込む処理に先立って、当該暗号化コンテンツ９０５が格納されているディレクトリ名をメモリカード９０２から取得し、当該取得されたディレクトリ名とＲＯＭ９１３に格納されている端末識別子９１４とが一致した場合には、当該取得したメモリカード９０２のディレクトリ名が、携帯電話機９０１によってメモリカード９０２に設定されたものであると判別することができる。

このように、メモリカード９０２に設定されているディレクトリ名が、携帯電話機９０１によってメモリカード９０２に設定されたものであることが判ると、暗号化/復号化プログラム９０９は、当該ディレクトリ名９０４が設定されたディレクトリ９０３に格納されている暗号化コンテンツ９０５を復号化し、当該復号化されたコンテンツ９１２をＲＡＭ９１１に格納する。

図１１は、携帯電話機９０１のＲＡＭ９１１に格納されているコンテンツ９１２を、メモリカード９０２に格納する際の、暗号化/復号化プログラム９０９の処理手順を示すフロー図である。

図１１に示すように、暗号化/復号化プログラム９０９は、ステップＳＴ１００１において、ＲＯＭ９１３から端末識別子９１４を取得する。そして、暗号化/復号化プログラム９０９は、ステップＳＴ１００２に移って、ステップＳＴ１００１において取得した端末識別子名のディレクトリ９０３がメモリカード９０２にあるか否かを判断する。

ここで否定結果が得られると、このことは、メモリカード９０２には、携帯電話機９０１によって設定されたディレクトリ９０３が存在しないことを意味しており、このとき、暗号化/復号化プログラム９０９は、ステップＳＴ１００３に移って、ＲＯＭ９１３に格納されている端末識別子名のディレクトリ９０３を作成し、ステップＳＴ１００４に移る。

これに対して、ステップＳＴ１００２において肯定結果が得られると、このことは、既に携帯電話機９０１によって作成されたディレクトリ９０３がメモリカード９０２に存在することを意味しており、このとき暗号化/復号化プログラム９０９はステップＳＴ１００４に移る。

ステップＳＴ１００４において、暗号化/復号化プログラム９０９は、ＲＡＭ９１１からコンテンツ９１２を取得した後、ステップＳＴ１００５に移って、ステップＳＴ１００４において取得したコンテンツ９１２を、ＲＯＭ１１３内の端末識別子９１４を用いて例えばトリプルＤＥＳ暗号方式で暗号化する。

そして、暗号化/復号化プログラム９０９は、ステップＳＴ１００６に移って、

ステップＳＴ１００５において暗号化された暗号化コンテンツ９０５を、ステップＳＴ１００３において作成されたディレクトリ９０３に格納する。

これにより、図１２に示すように、メモリカード９０２においては、それぞれ同じ端末識別子９１４によって暗号化されたコンテンツ９１２（暗号化コンテンツ９０５）、すなわち一つの携帯電話機９０１によって書き出された暗号化コンテンツ９０５が、当該携帯電話機固有の端末識別子名のディレクトリ９０３に格納された状態となる。

また、図１３は、図１１の処理手順によってメモリカード９０２に格納された暗号化コンテンツ９０５を携帯電話機９０１によって読み込んで復号化する際の、暗号化/復号化プログラム９０９とコンテンツ格納ディレクトリ判別プログラム９１０との処理手順を示すフロー図である。

図１３に示すように、コンテンツ格納ディレクトリ判別プログラム９１０は、ステップＳＴ１２０１において、メモリカード９０２内にディレクトリがあるか否かを調べる。ここで否定結果が得られると、このことは、メモリカード９０２には、読み込むべき暗号化コンテンツ９０５がないことを意味しており、このときコンテンツ格納ディレクトリ判別プログラム９１０は、この処理手順を終了する。

これに対して、ステップＳＴ１２０１において肯定結果が得られると、このことは、メモリカード９０２には、読み込むべき暗号化コンテンツ９０５があることを意味しており、このときコンテンツ格納ディレクトリ判別プログラム９１０は、ステップＳＴ１２０２に移って、メモリ読込プログラム１０８を用いてメモリカード９０２からディレクトリ名を取得した後、ステップＳＴ１２０３に移る。ステップＳＴ１２０３において、コンテンツ格納ディレクトリ判別プログラム９１０は、ステップＳＴ１２０２において取得したディレクトリ名が、ＲＯＭ９１３に格納されている端末識別子９１４と同一であるか否かを判断する。

ここで否定結果が得られると、このことは、このときメモリカード９０２か

ら取得したディレクトリ名が、携帯電話機９０１によって設定されたディレクトリ９０４ではないこと、すなわち、そのディレクトリに格納されている暗号化コンテンツは、携帯電話機９０１によって利用できないものであることを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム９１０は、当該不一致の結果を暗号化/復号化プログラム９０９に通知するとともに、上述のステップＳＴ１２０１に戻って、メモリカード９０２内に次のディレクトリがあるか否かを判断し、次のディレクトリがある場合には、そのディレクトリについて同様の処理を実行する。

これに対して、ステップＳＴ１２０３において肯定結果が得られると、このことは、このとき取得したディレクトリが、携帯電話機９０１によって設定されたもの、すなわち、そのディレクトリに格納されている暗号化コンテンツは、携帯電話機９０１によって利用できるものであることを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム９１０は、当該一致の結果を暗号化/復号化プログラム９０９に通知するとともに、ステップＳＴ１２０４に移る。

ステップＳＴ１２０４において、コンテンツ格納ディレクトリ判別プログラム９１０は、上述のステップＳＴ１２０３において一致結果が得られたディレクトリ９０４の情報、または当該ディレクトリに格納されている暗号化コンテンツ９０５に関する情報（例えばタイトル等）を、液晶画面１１６に一覧表示する。

これにより、液晶画面１１６には、メモリカード９０２に格納されている暗号化コンテンツのうち、携帯電話機９０１によって利用可能な暗号化コンテンツ９０５に関連する情報が表示される。

因みに、携帯電話機９０１によって利用可能な暗号化コンテンツ９０５に関する情報を一覧表示する構成としては、暗号化コンテンツ９０５をメモリカード９０２に格納する際に、その暗号化コンテンツ９０５に対応したタイトル等の簡易情報のみを携帯電話機９０１のＲＡＭ９１１に格納し、ステップＳＴ１

２０３における一致結果に基づいて、当該格納されている簡易情報を一覧表示する等の方法も考えられる。

ステップＳＴ１２０４において、液晶画面１１６にコンテンツの一覧が表示されると、利用者は、入力インターフェイス１１７を操作することにより、当該表示された一覧のなかから所望とするコンテンツを選択する。

これにより、暗号化/復号化プログラム９０９は、ステップＳＴ１２０５に移って、メモリ読込プログラム１０８を用いて、このとき入力インターフェイス１１７を介して指定された暗号化コンテンツ９０５をメモリカード９０２から読み込み、さらに続くステップＳＴ１２０６に移って、ステップＳＴ１２０５においてメモリカード９０２から取得した暗号化コンテンツ９０５を、ＲＯＭ９１３に格納されている端末識別子９１４を用いて復号化し、ＲＡＭ９１１に格納する。

ＲＡＭ９１１に格納されたコンテンツ９１２は、携帯電話機９０１の利用者が入力インターフェイス１１７を操作することにより起動され、利用者の利用に供される。

以上の構成において、携帯電話機９０１は、メモリカード９０２に暗号化コンテンツ９０５を書き出す際に、当該暗号化コンテンツ９０５を格納するディレクトリ９０４の名前として、当該携帯電話機９０１に固有の端末識別子９１４を用いる。

このディレクトリ名は、暗号化コンテンツ９０５に比べてそのデータ量は格段に少ないものとなっている。従って、携帯電話機９０１は、メモリカード９０２から暗号化コンテンツ９０５を読み込んで復号化する前に、当該暗号化コンテンツ９０５が格納されたディレクトリ９０４のディレクトリ名を読み込んで、当該ディレクトリ名が携帯電話機９０１の端末識別子９１４と一致するか否かを判別する。

ディレクトリ名が携帯電話機９０１の端末識別子９１４と一致する場合、当該ディレクトリ名が付けられたディレクトリ９０４に格納されている暗号化

コンテンツ９０５は、携帯電話機９０１によってメモリカード９０２に書き出されたものであることになる。

従って、この暗号化コンテンツ９０５は、携帯電話機９０１に読み込んで、当該携帯電話機９０１によって利用することが可能であり、携帯電話機９０１の暗号化/復号化プログラム９０９は、メモリカード９０２から暗号化コンテンツ９０５を読み込み、当該読み込まれた暗号化コンテンツ９０５を復号化する。

このように、ディレクトリ名が、ＲＯＭ９１３に格納されている端末識別子９１４と一致することを条件に、当該ディレクトリ名が付けられたディレクトリ９０４に格納されている暗号化コンテンツ９０５をメモリカード９０２から携帯電話機９０１に読み込んで復号化することにより、携帯電話機９０１は、当該携帯電話機９０１において利用可能である暗号化コンテンツ９０５のみを選択的に復号化することができる。

従って、メモリカード９０２に複数の暗号化コンテンツが格納されている状態であって、これら複数の暗号化コンテンツを利用可能な端末装置（携帯電話機等）が各暗号化コンテンツ毎に異なる場合であっても、携帯電話機９０１は、これら複数のデータ量の多い暗号化コンテンツをすべて復号化する必要はなく、当該複数の暗号化コンテンツにそれぞれ対応付けられた、データ量の少ないディレクトリを取得するだけで、利用可能な暗号化コンテンツ９０５を判別することができる。

このように、本実施の形態のコンテンツ処理装置としての携帯電話機９０１によれば、コンテンツ蓄積媒体であるメモリカード９０２に格納された複数の暗号化コンテンツの判別を一段と容易に行うことが可能となり、携帯電話機９０１において利用可能な暗号化コンテンツ９０５を一段と迅速に復号化することができる。また、本実施の形態のコンテンツ処理装置としての携帯電話機９０１によれば、ＲＯＭ９１３に格納された端末識別子９１４をそのままメモリカード９０２のディレクトリ名として用いることにより、一段と簡単な構成によって暗号化コンテンツ９０５の判別を行うことができる。

なお、この実施の形態においては、コンテンツを格納するコンテンツ蓄積媒体としてメモリカード９０２を用いる場合について述べたが、これに限らず、要はデジタル情報化されたコンテンツを格納可能なコンテンツ蓄積媒体であれば、他のデバイスを広く適用することができる。

（実施の形態４）

図１４は、本発明の実施の形態４に係るコンテンツ処理装置としての携帯電話機１３０１の構成を示すブロック図である。但し、図１及び図２と同一の構成となるものについては、図１及び図２と同一番号を付し、詳しい説明を省略する。

この図１４に示される携帯電話機１３０１は、認証プログラム１３０９を有し、当該認証プログラム１３０９によって認証を行うことによりアクセスが可能となる認証領域１３０３をメモリカード１３０２に設け、当該認証領域１３０３に端末装置（携帯電話機１３０１）に固有の端末識別子１３１７を格納するようにした点が図２の構成の携帯電話機１０１と異なる。

図２との対応部分に同一符号を付して示す図１４は、携帯電話機１３０１の構成を示すブロック図である。この図１４は、携帯電話機１３０１の構成のうち、特にコンテンツ処理に関わる構成を抽出して示すものである。携帯電話機１３０１は、それぞれ図示しないＣＰＵ（Central Processing Unit）によって動作するメモリ書出プログラム１０７、メモリ読込プログラム１０８、暗号化/復号化プログラム１３１２、コンテンツ格納ディレクトリ判別プログラム１３１３及び認証プログラム１３０９を含んでいる。

図１４において、携帯電話機１３０１は、コンテンツプロバイダから携帯電話回線網を介してダウンロードしたコンテンツ１３１５をＲＡＭ（Random Access Memory）１３１４に格納する。暗号化/復号化プログラム１３１２は、ＲＡＭ１３１４に格納されたコンテンツ１３１５を暗号化するものであり、当該暗号化/復号化プログラム１３１２によって暗号化されたコンテンツ１３１５は、暗号化コンテンツ１３０７として、メモリ書出プログラム１０７によっ

てメモリカードインターフェイス１０６を介してメモリカード１３０２の通常領域１３０５に書き込まれる。通常領域１３０５は、携帯電話機１３０１に設けられた認証プログラム１３０９の認証処理を必要とせずにアクセス可能な領域である。

ＲＯＭ（Read Only Memory）１３１６は、携帯電話機１３０１に固有の、例えば電話番号等でなる端末識別子１３１７を格納している。

暗号化/復号化プログラム１３１２は、コンテンツ１３１５を暗号化する際、ＲＯＭ（Read Only Memory）１３１６に格納されている端末識別子１３１７を用いて暗号化する。また、暗号化/復号化プログラム１３１２は、コンテンツ１３１５を暗号化してメモリカード１３０２に格納する処理に伴って、ＲＯＭ１３１６に格納されている端末識別子１３１７を、メモリ書出プログラム１０７によってメモリカード１３０２の認証領域１３０３に格納する。この認証領域１３０３における端末識別子１３１７は、通常領域１３０５の暗号化コンテンツ１３０７が格納されるディレクトリと同じディレクトリに格納されるリンク情報１３０８によって暗号化コンテンツ１３０７と対応付けられる。このように、端末識別子１３１７及び暗号化コンテンツ１３０７は、リンク情報１３０８によって対応付けられて、認証領域１３０３及び通常領域１３０５に分けて格納される。

また、メモリカード１３０２に格納された暗号化コンテンツ１３０７を携帯電話機１３０１に読み込む場合、携帯電話機１３０１のメモリ読込プログラム１０８は、暗号化コンテンツ１３０７を読み込む処理に先立って、当該暗号化コンテンツ１３０７と同じディレクトリに格納されているリンク情報１３０８によって対応付けられた、認証領域１３０３の端末識別子１３１７をメモリカード１３０２からメモリカードインターフェイス１０６を介して読み込む。

当該読み込まれた端末識別子１３１７は、コンテンツ格納ディレクトリ判別プログラム１３１３によって、ＲＯＭ１３１６に格納されている携帯電話機１３０１に固有の端末識別子１３１７と比較し、当該比較結果として一致結果が

得られた場合には、メモリカード１３０２の端末識別子１３１７が、携帯電話機１３０１によってメモリカード１３０２に書き込まれたものであると判別することができる。

このように、メモリカード１３０２に格納されている端末識別子１３１７が、携帯電話機１３０１によってメモリカード１３０２に書き込まれたものであることが判ると、暗号化/復号化プログラム１３１２は、メモリカード１３０２において端末識別子１３１７に対応付けられた、通常領域１３０５の暗号化コンテンツ１３０７を復号化し、当該復号化されたコンテンツ１３１５をＲＡＭ１３１４に格納する。

図１５は、携帯電話機１３０１のＲＡＭ１３１４に格納されているコンテンツ１３１５を、メモリカード１３０２に格納する際の、認証プログラム１３０９及び暗号化/復号化プログラム１３１２の処理手順を示すフロー図である。

図１５に示すように、認証プログラム１３０９は、ステップＳＴ１４０１において、まず、メモリカード１３０２との間で認証を行う。因みに、メモリカード１３０２には、図示しない認証プログラムが設けられており、携帯電話機１３０１の認証プログラム１３０９との間で認証処理を行い、当該認証結果として携帯電話機１３０１がメモリカード１３０２の認証領域１３０３にアクセス可能な端末装置であるという結果が得られると、認証領域１３０３へのアクセスを許可するようになされている。

ステップＳＴ１４０１における認証処理の結果として、携帯電話機１３０１からメモリカード１３０２の認証領域１３０３へのアクセスが可能になると、認証プログラム１３０９は、当該認証結果を暗号化/復号化プログラム１３１２に通知する。この通知を受け取った暗号化/復号化プログラム１３１２は、ステップＳＴ１４０２において、ＲＯＭ１３１６から端末識別子１３１７を取得する。そして、暗号化/復号化プログラム１３１２は、ステップＳＴ１４０３に移って、このときメモリカードインターフェイス１０６に装着されているメモリカード１３０２の認証領域１３０３に、ステップＳＴ１４０２においてＲＯＭ

１３１６から取得した端末識別子１３１７と同じ端末識別子が既に格納されているか否かを判断する。ここで否定結果が得られると、このことは、メモリカード１３０２には、携帯電話機１３０１によって書き出された端末識別子１３１７が格納されていないことを意味しており、このとき暗号化/復号化プログラム１３１２は、ステップＳＴ１４０４に移って、ステップＳＴ１４０２において取得した端末識別子１３１７とリンク情報１３０８を、メモリ書出プログラム１０７を用いてメモリカード１３０２に格納した後、ステップＳＴ１４０５に移る。この場合、暗号化/復号化プログラム１３１２は、端末識別子１３１７を認証領域１３０３に格納するとともに、リンク情報１３０８を通常領域１３０５のコンテンツ格納ディレクトリ１３０６に格納する。リンク情報１３０８は、認証領域１３０３に格納された端末識別子１３１７と、これに対応付けられた、通常領域１３０５のコンテンツ格納ディレクトリ１３０６に格納される暗号化コンテンツ１３０７とを対応付けるための情報である。

また、ステップＳＴ１４０３において肯定結果が得られると、このことは、メモリカード１３０２には、携帯電話機１３０１によって書き出された端末識別子１３１７が格納されていることを意味しており、このとき暗号化/復号化プログラム１３１２は、ステップＳＴ１４０５に移る。

ステップＳＴ１４０５において、暗号化/復号化プログラム１３１２は、ＲＡＭ１３１４からコンテンツ１３１５を取得した後、ステップＳＴ１４０６に移って、ステップＳＴ１４０５において取得したコンテンツ１３１５を、ＲＯＭ１３１６内の端末識別子１３１７を用いて例えばトリプルＤＥＳ暗号方式で暗号化する。

そして、暗号化/復号化プログラム１３１２は、ステップＳＴ１４０７に移って、ステップＳＴ１４０６において暗号化された暗号化コンテンツ１３０７を、ステップＳＴ１４０４においてメモリカード１３０２に格納された端末識別子１３１７とリンク情報１３０８によって対応付けられたディレクトリに格納する。

これにより、図１６に示すように、メモリカード１３０２においては、それぞれ同じ端末識別子１３１７によって暗号化されたコンテンツ１３１５（暗号化コンテンツ１３０７）と端末識別子１３１７とが、リンク情報１３０８によって対応付けられて格納された状態となる。このように、暗号化コンテンツ１３０７と端末識別子１３１７とをリンク情報１３０８によって対応付けるとともに、暗号化コンテンツ１３０７の存在を確認するための端末識別子１３１７を認証領域１３０３に格納することにより、認証領域１３０３にアクセスが可能な携帯電話機１３０１のみによって暗号化コンテンツ１３０７の存在を確認することが可能な状態となる。

また、図１７は、図１５の処理手順によってメモリカード１３０２に格納された暗号化コンテンツ１３０７と端末識別子１３１７とを携帯電話機１３０１によって読み込んで復号化する際の、暗号化/復号化プログラム１３１２とコンテンツ格納ディレクトリ判別プログラム１３１３との処理手順を示すフロー図である。

図１７に示すように、コンテンツ格納ディレクトリ判別プログラム１３１３は、ステップＳＴ１６０１において、メモリカード１３０１の通常領域１３０５にリンク情報１３０８があるか否かを判断する。ここで否定結果が得られると、このことは、リンク情報１３０８がメモリカード１３０２に格納されていないこと、すなわち、暗号化コンテンツ１３０７が格納されていないことを意味しており、このときコンテンツ格納ディレクトリ判別プログラム１３１３は、当該処理手順を終了する。

これに対して、ステップＳＴ１６０１において肯定結果が得られると、このことは、リンク情報１３０８がメモリカード１３０２に格納されていること、すなわち、暗号化コンテンツ１３０７が存在することを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム１３１３は、ステップＳＴ１６０２に移って、認証プログラム１３０９による認証処理を行った上で、メモリ読込プログラム１０８を用いてメモリカード１３０２から、リンク情報１３

０８に対応する端末識別子１３１７を認証領域１３０３から取得する。

そして、コンテンツ格納ディレクトリ判別プログラム１３１３は、ステップＳＴ１６０３に移って、ステップＳＴ１６０２において取得した端末識別子と、ＲＯＭ１３１６に格納されている端末識別子１３１７とを比較し、取得した端末識別子と、ＲＯＭ１３１６に格納されている端末識別子１３１７とが同一であるか否かを判断する。

因みに、携帯電話機１３０１は、コンテンツ１３１５を暗号化してメモリカード１３０２に書き出す場合には、常に、端末識別子１３１７を、暗号化コンテンツ１３０７に対応付けて格納するようになっている。従って、ステップＳＴ１６０２において取得された端末識別子と、ＲＯＭ１３１６に格納されている端末識別子１３１７との比較結果が一致する場合、このことは、このときメモリカード１３０２から取得された端末識別子が携帯電話機１３０１によってメモリカード１３０２に書き出されたもの、すなわち、当該端末識別子１３１７とリンク情報１３０８によって対応付けられてメモリカード１３０２に格納されている暗号化コンテンツ１３０７が携帯電話機１３０１によってメモリカード１３０２に書き出されたものであることを意味する。

従って、ステップＳＴ１６０２においてメモリカード１３０２から取得された端末識別子１３１７と、ＲＯＭ１３１６に格納されている端末識別子１３１７との比較結果が一致する場合、コンテンツ格納ディレクトリ判別プログラム１３１３は、当該一致結果を暗号化/復号化プログラム１３１２に通知するとともに、ステップＳＴ１６０３からテップＳＴ１６０４に移る。

これに対して、ステップＳＴ１６０２においてメモリカード１３０２から取得された端末識別子と、ＲＯＭ１３１６に格納されている端末識別子１３１７との比較結果が一致しない場合、コンテンツ格納ディレクトリ判別プログラム１３１３は、当該不一致の結果を暗号化/復号化プログラム１３１２に通知するとともに、上述のステップＳＴ１６０１に戻って、メモリカード１３０２内に次のリンク情報１３０８があるか否かを判断し、次のリンク情報１３０８があ

る場合には、そのリンク情報１３０８について同様の処理を実行する。

ステップＳＴ１６０４において、コンテンツ格納ディレクトリ判別プログラム１３１３は、上述のステップＳＴ１６０３において一致結果が得られた端末識別子１３１７の情報、または、当該端末識別子１３１７にリンク情報１３０８によって対応付けられたディレクトリ１３０６に格納されている暗号化コンテンツ１３０７に関する情報を液晶画面１１６に一覧表示する。

これにより、液晶画面１１６には、メモリカード１３０２に格納されている暗号化コンテンツのうち、携帯電話機１３０１によって利用可能な暗号化コンテンツ１３０７に関連する情報が一覧表示される。

因みに、携帯電話機１３０１によって利用可能な暗号化コンテンツ１３０７に関する情報を一覧表示する構成としては、暗号化コンテンツ１３０７をメモリカード１３０２に格納する際に、その暗号化コンテンツ１３０７に対応したタイトル等の簡易情報のみを携帯電話機１３０１のＲＡＭ１３１４に格納し、ステップＳＴ１６０３における一致結果に基づいて、当該格納されている簡易情報を一覧表示する等の方法も考えられる。

ステップＳＴ１６０４において、液晶画面１１６にコンテンツの一覧が表示されると、利用者は、入力インターフェイス１１７を操作することにより、当該表示された一覧のなかから所望とするコンテンツを選択する。

これにより、暗号化/復号化プログラム１３１２は、ステップＳＴ１６０５に移って、メモリ読込プログラム１０８を用いて、このとき入力インターフェイス１１７を介して指定された暗号化コンテンツ１３０７をメモリカード１３０２から読み込み、さらに続くステップＳＴ１６０６に移って、ステップＳＴ１６０５においてメモリカード１３０２から取得した暗号化コンテンツ１３０７を、ＲＯＭ１３１６に格納されている端末識別子１３１７を用いて復号化し、ＲＡＭ１３１４に格納する。

ＲＡＭ１３１４に格納されたコンテンツ１３１５は、携帯電話機１３０１の利用者が入力インターフェイス１１７を操作することにより起動され、利用者

の利用に供される。

以上の構成において、携帯電話機１３０１は、メモリカード１３０２に暗号化コンテンツ１３０７を書き出す際に、当該暗号化コンテンツ１３０７に対応付けられた端末識別子１３１７をメモリカード１３０２の認証領域１３０３に格納しておく。

この端末識別子１３１７は、例えば、携帯電話機１３０１の電話番号等であり、暗号化コンテンツ１３０７に比べてそのデータ量は格段に少ないものとなっている。従って、携帯電話機１３０１は、メモリカード１３０２から暗号化コンテンツ１３０７を読み込んで復号化する前に、当該暗号化コンテンツ１３０７に対応付けられた端末識別子１３１７をメモリカード１３０２から読み込み、当該端末識別子１３１７が携帯電話機１３０１によってメモリカード１３０２に書き出されたものであるか否かを判別することにより、データ量の少ない端末識別子１３１７に基づいて、携帯電話機１３０１において利用可能なコンテンツが、メモリカード１３０２に存在するか否かを容易に判断することができる。

この実施の形態の場合、端末識別子１３１７は、認証領域１３０３に格納されていることにより、携帯電話機１３０１からメモリカード１３０２の認証領域１３０３へのアクセスは、認証処理を行った上で実行される。従って、認証領域１３０３へのアクセスが可能な携帯電話機１３０１以外の端末装置では、端末識別子１３１７の取得が困難となることにより、利用可能である暗号化コンテンツの判別を容易に行うことは困難となる。

このように、本実施の形態のコンテンツ処理装置としての携帯電話機１３０１によれば、コンテンツ蓄積媒体であるメモリカード１３０２に格納された複数の暗号化コンテンツの判別を、認証が可能な携帯電話機１３０１においてのみ一段と容易に行うことが可能となる。

なお、この実施の形態においては、携帯電話機１３０１のＲＯＭ１３１６に格納されている端末識別子１３１７を、暗号化せずにメモリカード１３０２の

認証領域１３０３に格納する場合について述べたが、これに限らず、暗号化した後にメモリカード１３０２の認証領域１３０３に格納するようにしてもよい。

また、この実施の形態においては、携帯電話機１３０１のＲＯＭ１３１６に格納されている端末識別子１３１７をそのまま、メモリカード１３０２の認証領域１３０３に格納する場合について述べたが、これに限らず、端末識別子１３１７を所定の変換式によって変換したものを認証領域１３０３に格納するとともに、当該認証領域１３０３から当該変換されたものを携帯電話機１３０１に読み込んでこれを逆変換式によって逆変換し、ＲＯＭ１３１６の端末識別子１３１７と比較するようにしてもよい。この場合、変換式としては、端末識別子１３１７の特定の位置（例えば下４桁）を抜き出したり、または、端末識別子１３１７の文字列を並び替える等、種々の変換式を用いることができる。

なお、この実施の形態の携帯電話機１３０１においては、端末識別子１３１７として、その携帯電話機１３０１の電話番号を用いる場合について述べたが、これに限らず、例えば携帯電話機１３０１の製造番号のようなその携帯電話機１３０１を識別するための識別子、又は、その他の何らかの意味を持つ文字列、数値、画像または音声等のデータ、若しくは特定のサービスと契約したことを示す識別子（会員番号等）を用いるようにしてもよい。また、この端末識別子１３１７として電話番号、製造番号、又はその他の文字列等の情報そのものではなく、端末識別子に対してある変換を加えた結果（端末識別子に関連する情報）を用いるようにしてもよい。このようにすれば、端末識別子によってコンテンツを暗号化する際の暗号化方法、及び端末識別子が第三者に漏洩した場合であっても、その端末識別子は、暗号化鍵となり得る他のデータに変換されていることにより、このデータ（暗号化鍵）によって暗号化された暗号化コンテンツが解読されることを防止することができる。

また、この実施の形態においては、コンテンツ１３１５を端末識別子１３１７を用いて暗号化し、メモリカード１３０２に格納する場合について述べたが、

これに限らず、コンテンツ１３１５を端末識別子１３１７に関連する情報を用いて暗号化するようにしてもよい。

また、この実施の形態においては、通常領域に格納されたリンク情報によって認証領域の端末識別子を特定する場合について述べたが、これに限らず、例えば、通常領域に格納されている暗号化コンテンツの当該通常領域での格納位置を示す情報（ルート名、ディレクトリ名等）と、これに対応して認証領域に格納されている端末識別子の当該認証領域での格納位置を示す情報（ルート名、ディレクトリ名等）を同一とするようにしてもよい。このように同じディレクトリ構成とすれば、リンク情報を用いることなく認証領域での端末識別子と通常領域の暗号化コンテンツとを対応付けることができる。

また、この実施の形態においては、コンテンツを格納するコンテンツ蓄積媒体としてメモリカード１３０２を用いる場合について述べたが、これに限らず、要はデジタル情報化されたコンテンツを格納可能なコンテンツ蓄積媒体であれば、他のデバイスを広く適用することができる。

（実施の形態５）

図１８は、本発明の実施の形態５に係るコンテンツ処理装置としての携帯電話機１７０１の構成を示すブロック図である。但し、図１及び図２と同一の構成となるものについては、図１及び図２と同一番号を付し、詳しい説明を省略する。

この図１８に示される携帯電話機１７０１は、ＲＯＭ１７１３に格納される端末識別子として、コンテンツ１７１２を暗号化するための暗号化用端末識別子１７１４と、メモリカード１７０２内の暗号化コンテンツを格納するコンテンツ格納ディレクトリ（以下、これを単にディレクトリと称する）１７０３のディレクトリ名１７０４として用いるディレクトリ判別用端末識別子１７１５とを用意した点が図２の構成の携帯電話機１０１と異なる。

図２との対応部分に同一符号を付して示す図１８は、携帯電話機１７０１の構成を示すブロック図である。この図１８は、携帯電話機１７０１の構成のう

ち、特にコンテンツ処理に関わる構成を抽出して示すものである。携帯電話機１７０１は、それぞれ図示しないＣＰＵ（Central Processing Unit）によって動作するメモリ書出プログラム１０７、メモリ読込プログラム１０８、暗号化/復号化プログラム１７０９及びコンテンツ格納ディレクトリ判別プログラム１７１０を含んでいる。

図１８において、携帯電話機１７０１は、コンテンツプロバイダから携帯電話回線網を介してダウンロードしたコンテンツ１７１２をＲＡＭ（Random Access Memory）１７１１に格納する。暗号化/復号化プログラム１７０９は、ＲＡＭ１７１１に格納されたコンテンツ１７１２を暗号化するものであり、当該暗号化/復号化プログラム１７０９によって暗号化されたコンテンツ１７１２は、暗号化コンテンツ１７０５として、メモリ書出プログラム１０７によってメモリカードインターフェイス１０６を介してメモリカード１７０２に書き込まれる。

ＲＯＭ（Read Only Memory）１７１３は、携帯電話機１７０１に固有の所定の文字列（製造番号等）でなる識別子であって、コンテンツ１７１２を暗号化する際に用いられる暗号化用端末識別子１７１４と、携帯電話機１７０１に固有の所定の文字列（電話番号等）でなる識別子であって、暗号化コンテンツをメモリカード１７０２に格納する際に用いられるディレクトリ名１７０４となるディレクトリ判別用端末識別子１７１５を格納している。暗号化用端末識別子１７１４とディレクトリ判別用端末識別子１７１５とは、互いに異なる文字列が用いられる。

暗号化/復号化プログラム１７０９は、コンテンツ１７１２を暗号化する際、ＲＯＭ（Read Only Memory）１７１３に格納されている暗号化用端末識別子１７１４を用いて暗号化する。また、暗号化/復号化プログラム１７０９は、当該暗号化されたコンテンツ１７１２（暗号化コンテンツ１７０５）をメモリカード１７０２に格納する際、当該格納先となるディレクトリ１７０３のディレクトリ名１７０４を、ＲＯＭ１７１３に格納されているディレクトリ判別用端

末識別子１７１５の端末識別子名とする。

また、メモリカード１７０２に格納された暗号化コンテンツ１７０５を携帯電話機１７０１に読み込む場合、携帯電話機１７０１のメモリ読込プログラム１０８は、暗号化コンテンツ１７０５を読み込む処理に先立って、当該暗号化コンテンツ１７０５が格納されているディレクトリ名１７０４をメモリカード１７０２から取得し、当該取得されたディレクトリ名１７０４とＲＯＭ１７１３に格納されているディレクトリ判別用端末識別子１７１５とが一致した場合には、当該取得したメモリカード１７０２のディレクトリ名１７０４が、携帯電話機１７０１によってメモリカード１７０２に設定されたものであると判別することができる。

このように、メモリカード１７０２に設定されているディレクトリ名１７０４が、携帯電話機１７０１によってメモリカード１７０２に設定されたものであることが判ると、暗号化/復号化プログラム１７０９は、当該ディレクトリ名１７０４によって表わされるディレクトリ１７０３に格納されている暗号化コンテンツ１７０５を復号化し、当該復号化されたコンテンツ１７１２をＲＡＭ１７１１に格納する。

図１９は、携帯電話機１７０１のＲＡＭ１７１１に格納されているコンテンツ１７１２を、メモリカード１７０２に格納する際の、暗号化/復号化プログラム１７０９の処理手順を示すフロー図である。

図１９に示すように、暗号化/復号化プログラム１７０９は、ステップＳＴ１８０１において、ＲＯＭ１７１３からディレクトリ判別用端末識別子１７１５を取得する。そして、暗号化/復号化プログラム１７０９は、ステップＳＴ１８０２に移って、ステップＳＴ１８０１において取得したディレクトリ判別用端末識別子１７１５の識別子名と同じディレクトリ名１７０４のディレクトリ１７０３がメモリカード１７０２にあるか否かを判断する。

ここで否定結果が得られると、このことは、メモリカード１７０２には、携帯電話機１７０１によって設定されたディレクトリ１７０３が存在しないこ

とを意味しており、このとき、暗号化/復号化プログラム１７０９は、ステップＳＴ１８０３に移って、ＲＯＭ１７１３に格納されているディレクトリ判別用端末識別子１７１５の識別子名と同じディレクトリ名１７０４のディレクトリ１７０３を作成し、ステップＳＴ１８０４に移る。

これに対して、ステップＳＴ１８０２において肯定結果が得られると、このことは、既に携帯電話機１７０１によって作成されたディレクトリ１７０３がメモリカード１７０２に存在することを意味しており、このとき暗号化/復号化プログラム１７０９はステップＳＴ１８０４に移る。

ステップＳＴ１８０４において、暗号化/復号化プログラム１７０９は、ＲＡＭ１７１１からコンテンツ１７１２を取得した後、ステップＳＴ１８０５に移って、ステップＳＴ１８０４において取得したコンテンツ１７１２を、ＲＯＭ１７１３内の暗号化端末識別子１７１４を用いて例えばトリプルＤＥＳ暗号方式で暗号化する。

そして、暗号化/復号化プログラム１７０９は、ステップＳＴ１８０６に移って、ステップＳＴ１８０５において暗号化された暗号化コンテンツ１７０５を、ステップＳＴ１８０３において作成されたディレクトリ名１７０４のディレクトリ１７０３に格納する。

これにより、図２０に示すように、メモリカード１７０２においては、それぞれ同じ暗号化用端末識別子１７１４によって暗号化されたコンテンツ１７１２（暗号化コンテンツ１７０５）、すなわち一つの携帯電話機１７０１によって書き出された暗号化コンテンツ１７０５が、当該携帯電話機固有の端末識別子名と同じディレクトリ名１７０４のディレクトリ１７０３に格納された状態となる。

また、図２１は、図１９の処理手順によってメモリカード１７０２に格納された暗号化コンテンツ１７０５を携帯電話機１７０１によって読み込んで復号化する際の、暗号化/復号化プログラム１７０９とコンテンツ格納ディレクトリ判別プログラム１７１０との処理手順を示すフロー図である。

図２１に示すように、コンテンツ格納ディレクトリ判別プログラム１７１０は、ステップＳＴ２００１において、メモリカード１７０２内にディレクトリがあるか否かを調べる。ここで否定結果が得られると、このことは、メモリカード１７０２には、読み込むべき暗号化コンテンツ１７０５がないことを意味しており、このときコンテンツ格納ディレクトリ判別プログラム１７１０は、この処理手順を終了する。

これに対して、ステップＳＴ２００１において肯定結果が得られると、このことは、メモリカード１７０２には、読み込むべき暗号化コンテンツ１７０５があることを意味しており、このときコンテンツ格納ディレクトリ判別プログラム１７１０は、ステップＳＴ２００２に移って、メモリ読込プログラム１０８を用いてメモリカード１７０２からディレクトリ名を取得した後、ステップＳＴ２００３に移る。ステップＳＴ２００３において、コンテンツ格納ディレクトリ判別プログラム１７１０は、ステップＳＴ２００２において取得したディレクトリ名が、ＲＯＭ１７１３に格納されているディレクトリ判別用端末識別子１７１５と同一であるか否かを判断する。

ここで否定結果が得られると、このことは、このときメモリカード１７０２から取得したディレクトリ名が、携帯電話機１７０１によって設定されたディレクトリ名１７０４ではないこと、すなわち、そのディレクトリに格納されている暗号化コンテンツは、携帯電話機１７０１によって利用できないものであることを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム１７１０は、当該不一致の結果を暗号化/復号化プログラム１７０９に通知するとともに、上述のステップＳＴ２００１に戻って、メモリカード１７０２内に次のディレクトリがあるか否かを判断し、次のディレクトリがある場合には、そのディレクトリについて同様の処理を実行する。

これに対して、ステップＳＴ２００３において肯定結果が得られると、このことは、このとき取得したディレクトリ名が、携帯電話機１７０１によって設定されたもの、すなわち、そのディレクトリ１７０３に格納されている暗号化

コンテンツ１７０５は、携帯電話機１７０１によって利用できるものであることを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム１７１０は、当該一致の結果を暗号化/復号化プログラム１７０９に通知するとともに、ステップＳＴ２００４に移る。

ステップＳＴ２００４において、コンテンツ格納ディレクトリ判別プログラム１７１０は、上述のステップＳＴ２００３において一致結果が得られたディレクトリ名１７０４に関する情報、または、当該ディレクトリ名１７０４のディレクトリ１７０３に格納されている暗号化コンテンツ１７０５に関連する情報を液晶画面１１６に一覧表示する。

これにより、液晶画面１１６には、メモリカード１７０２に格納されている暗号化コンテンツのうち、携帯電話機１７０１によって利用可能な暗号化コンテンツ１７０５に関連する情報が一覧表示される。

因みに、携帯電話機１７０１によって利用可能な暗号化コンテンツ１７０５に関する情報を一覧表示する構成としては、暗号化コンテンツ１７０５をメモリカード１７０２に格納する際に、その暗号化コンテンツ１７０５に対応したタイトル等の簡易情報のみを携帯電話機１７０１のＲＡＭ１７１１に格納し、ステップＳＴ２００３における一致結果に基づいて、当該格納されている簡易情報を一覧表示する等の方法も考えられる。

ステップＳＴ２００４において、液晶画面１１６にコンテンツの一覧が表示されると、利用者は、入力インターフェイス１１７を操作することにより、当該表示された一覧のなかから所望とするコンテンツを選択する。

これにより、暗号化/復号化プログラム１７０９は、ステップＳＴ２００５に移って、メモリ読込プログラム１０８を用いて、このとき入力インターフェイス１１７を介して指定された暗号化コンテンツ１７０５をメモリカード１７０２から読み込み、さらに続くステップＳＴ２００６に移って、ステップＳＴ２００５においてメモリカード１７０２から取得した暗号化コンテンツ１７０５を、ＲＯＭ１７１３に格納されている暗号化用端末識別子１７１４を用い

て復号化し、ＲＡＭ１７１１に格納する。

ＲＡＭ１７１１に格納されたコンテンツ１７１２は、携帯電話機１７０１の利用者が入力インターフェイス１１７を操作することにより起動され、利用者の利用に供される。

以上の構成において、携帯電話機１７０１は、メモリカード１７０２に暗号化コンテンツ１７０５を書き出す際に、当該暗号化コンテンツ１７０５を格納するディレクトリのディレクトリ名１７０４として、当該携帯電話機１７０１に固有のディレクトリ判別用端末識別子１７１５を用いる。

このディレクトリ名は、暗号化コンテンツ１７０５に比べてそのデータ量は格段に少ないものとなっている。従って、携帯電話機１７０１は、メモリカード１７０２から暗号化コンテンツ１７０５を読み込んで復号化する前に、当該暗号化コンテンツ１７０５が格納されたディレクトリのディレクトリ名１７０４を読み込んで、当該ディレクトリ名が携帯電話機１７０１のディレクトリ判別用端末識別子１７１５と一致するか否かを判別する。

ディレクトリ名が携帯電話機１７０１のディレクトリ判別用端末識別子１７１５と一致する場合、当該ディレクトリ名１７０４が付けられたディレクトリに格納されている暗号化コンテンツ１７０５は、携帯電話機１７０１によってメモリカード１７０２に書き出されたものであることになる。

従って、この暗号化コンテンツ１７０５は、携帯電話機１７０１に読み込んで、当該携帯電話機１７０１によって利用することが可能であり、携帯電話機１７０１の暗号化/復号化プログラム１７０９は、メモリカード１７０２から暗号化コンテンツ１７０５を読み込み、当該読み込まれた暗号化コンテンツ１７０５を復号化する。

このように、ディレクトリ名が、ＲＯＭ１７１３に格納されているディレクトリ判別用端末識別子１７１５と一致することを条件に、当該ディレクトリ名１７０４が付けられたディレクトリに格納されている暗号化コンテンツ１７０５をメモリカード１７０２から携帯電話機１７０１に読み込んで復号化す

ることにより、携帯電話機１７０１は、当該携帯電話機１７０１において利用可能である暗号化コンテンツ１７０５のみを、データ量の少ないディレクトリ名に基づいて選択することができる。

従って、メモリカード１７０２に複数の暗号化コンテンツが格納されている状態であって、これら複数の暗号化コンテンツを利用可能な端末装置（携帯電話機等）が各暗号化コンテンツ毎に異なる場合であっても、携帯電話機１７０１は、これら複数のデータ量の多い暗号化コンテンツをすべて復号化する必要はなく、当該複数の暗号化コンテンツにそれぞれ対応付けられた、データ量の少ないディレクトリを取得するだけで、利用可能な暗号化コンテンツ１７０５を判別することができる。

また、ディレクトリ名１７０４として用いられるコンテンツ判別用端末識別子１７１４とは異なる暗号化用端末識別子１７１４によってコンテンツ１７１２を暗号化し、これをコンテンツ判別用端末識別子１７１４と同じディレクトリ名１７０４が付けられたディレクトリに格納することにより、ディレクトリ名１７０４が第三者に知られた場合であっても、暗号化コンテンツ１７０５が不正に復号化されることを防止することができる。

このように、本実施の形態のコンテンツ処理装置としての携帯電話機１７０１によれば、コンテンツ蓄積媒体であるメモリカード１７０２に格納された複数の暗号化コンテンツの判別を一段と容易に行うことが可能となり、携帯電話機１７０１において利用可能な暗号化コンテンツ１７０５を一段と迅速に復号化することができる。

なお、この実施の形態においては、携帯電話機１７０１のＲＯＭ１７１３に格納されているディレクトリ判別用端末識別子１７１５を暗号化せずに、メモリカード１７０２の暗号化コンテンツ格納用のディレクトリ名１７０４とした場合について述べたが、これに限らず、ディレクトリ判別用端末識別子１７１５を暗号化してディレクトリ名としてもよい。

また、この実施の形態においては、暗号化コンテンツ１７０５を格納するメ

モリカード１７０２のディレクトリ１７０４として、ディレクトリ判別用端末識別子１７１５を用いる場合について述べたが、これに限らず、図２について上述した特定データ１１５を用いるようにしてもよい。

また、この実施の形態の携帯電話機１７０１においては、暗号化用端末識別子１７１４及びディレクトリ判別用端末識別子１７１５として、電話番号、製造番号等を用いる場合について述べたが、これに限らず、何らかの意味を持つ文字列、数値、画像または音声等のデータ、若しくは特定のサービスと契約したことを示す識別子（会員番号等）を用いるようにしてもよい。また、この暗号化用端末識別子１７１４及びディレクトリ判別用端末識別子１７１５として電話番号、製造番号、又はその他の文字列等の情報そのものではなく、これらの端末識別子（暗号化用端末識別子１７１４及びディレクトリ判別用端末識別子１７１５）に対してそれぞれある変換を加えた結果（端末識別子に関連する情報）をそれぞれ用いるようにしてもよい。このようにすれば、端末識別子によってコンテンツを暗号化する際の暗号化方法、及び端末識別子が第三者に漏洩した場合であっても、その端末識別子は、暗号化鍵となり得る他のデータに変換されていることにより、このデータ（暗号化鍵）によって暗号化された暗号化コンテンツが解読されることを防止することができる。

また、この実施の形態においては、コンテンツ１７１２を暗号化用端末識別子１７１４を用いて暗号化し、メモリカード１７０２に格納する場合について述べたが、これに限らず、コンテンツ１７１２を暗号化用端末識別子１７１４に関連する情報を用いて暗号化するようにしてもよい。

また、この実施の形態においては、コンテンツを格納するコンテンツ蓄積媒体としてメモリカード１７０２を用いる場合について述べたが、これに限らず、要はデジタル情報化されたコンテンツを格納可能なコンテンツ蓄積媒体であれば、他のデバイスを広く適用することができる。

（実施の形態６）

図２２は、本発明の実施の形態６に係るコンテンツ処理装置としての携帯電

話機２１０１の構成を示すブロック図である。但し、図１及び図２と同一の構成となるものについては、図１及び図２と同一番号を付し、詳しい説明を省略する。

この図２２に示される携帯電話機２１０１は、ＲＡＭ２１１１に格納されているコンテンツ２１１２をメモリカード２１０２に書き出す際に、図２について上述した特定データ１１５に代えて、その書出し時刻を暗号化コンテンツ２１０５に対応付けて書き出す点が図２の構成の携帯電話機１０１と異なる。

図２との対応部分に同一符号を付して示す図２２は、携帯電話機２１０１の構成を示すブロック図である。この図２２は、携帯電話機２１０１の構成のうち、特にコンテンツ処理に関わる構成を抽出して示すものである。携帯電話機２１０１は、それぞれ図示しないＣＰＵ（Central Processing Unit）によって動作するメモリ書出プログラム１０７、メモリ読込プログラム１０８、暗号化/復号化プログラム２１０９、コンテンツ格納ディレクトリ判別プログラム２１１０及び時刻特定プログラム２１１９を含んでいる。

図２２において、携帯電話機２１０１は、コンテンツプロバイダから携帯電話回線網を介してダウンロードしたコンテンツ２１１２をＲＡＭ（Random Access Memory）２１１１に格納する。暗号化/復号化プログラム２１０９は、ＲＡＭ２１１１に格納されたコンテンツ２１１２を暗号化するものであり、当該暗号化/復号化プログラム２１０９によって暗号化されたコンテンツ２１１２は、暗号化コンテンツ２１０５として、メモリ書出プログラム１０７によってメモリカードインターフェイス１０６を介してメモリカード２１０２に書き込まれる。

ＲＯＭ（Read Only Memory）２１１４は、携帯電話機２１０１に固有の所定の文字列（電話番号等）でなる識別子であって、コンテンツ２１１２を暗号化する際に用いられる端末識別子２１１５を格納している。

暗号化/復号化プログラム２１０９は、コンテンツ２１１２を暗号化する際、ＲＯＭ（Read Only Memory）２１１３に格納されている端末識別子２１１５

を用いて暗号化する。また、暗号化/復号化プログラム２１０９は、当該暗号化されたコンテンツ２１１２（暗号化コンテンツ２１０５）をメモリカード２１０２に格納する際、時刻特定プログラム２１１９によって特定される書出時刻を表わす書出時刻情報２１１３を、メモリカード２１０２の暗号化コンテンツ２１０５が格納されたディレクトリと同じディレクトリに格納する。これにより、暗号化コンテンツ２１０５とその書出時刻情報２１１３とが対応付けられてメモリカード２１０２に格納された状態となる。また、メモリカード２１０２に格納された書出時刻情報２１１３は、暗号化/復号化プログラム２１０９及び時刻特定プログラム２１１９によって携帯電話機２１０１のＲＡＭ２１１１にも格納される。

また、メモリカード２１０２の所定のディレクトリ２１０３に格納された暗号化コンテンツ２１０５を携帯電話機２１０１に読み込む場合、携帯電話機２１０１のメモリ読込プログラム１０８は、暗号化コンテンツ２１０５を読み込む処理に先立って、携帯電話機２１０１のＲＡＭ２１１１に格納されている書出時刻情報２１１３と一致する書出時刻情報２１１３に対応付けられてメモリカード２１０２に格納されている暗号化コンテンツ２１０５を一覧情報化する。この一覧に載せられた暗号化コンテンツ２１０５は、携帯電話機２１０１によってメモリカード２１０２に書き出されたものであると判別することができる。

このように、メモリカード２１０２に格納されている書出時刻情報２１１３が、携帯電話機２１０１によってメモリカード２１０２に格納されたものであることが判ると、暗号化/復号化プログラム２１０９は、当該書出時刻情報２１１３に対応付けられて格納されている暗号化コンテンツ２１０５を復号化し、当該復号化されたコンテンツ２１１２をＲＡＭ２１１１に格納する。

図２３は、携帯電話機２１０１のＲＡＭ２１１１に格納されているコンテンツ２１１２を、メモリカード２１０２に格納する際の、暗号化/復号化プログラム２１０９及び時刻特定プログラム２１１９の処理手順を示すフロー図であ

る。

図２３に示すように、暗号化/復号化プログラム２１０９は、ステップＳＴ２２０１において、まず、コンテンツ格納用のディレクトリ２１０３を作成した後、続くステップＳＴ２２０２に移って、ＲＡＭ２１１１からコンテンツ２１１２を取得する。そして、暗号化/復号化プログラム２１０９は、ステップＳＴ２２０３に移って、ステップＳＴ２２０２において取得したコンテンツ２１１２を、ＲＯＭ２１１４内の端末識別子２１１５を用いて例えばトリプルＤＥＳ暗号方式で暗号化する。

そして、暗号化/復号化プログラム２１０９は、ステップＳＴ２２０４に移って、このときの時刻情報を時刻特定プログラム２１１９によって生成し、これを書出時刻情報２１１３としてＲＡＭ２１１１に格納する。これにより、ＲＡＭ２１１１には、暗号化コンテンツ２１０５をメモリカード２１０２に書き出す際の書出時刻情報２１１３が格納される。

そして、暗号化/復号化プログラム２１０９は、ステップＳＴ２２０５に移って、ステップＳＴ２２０３において暗号化された暗号化コンテンツ２１０５を、ステップＳＴ２２０４において生成された書出時刻情報２１１３とともに、ステップＳＴ２２０１において作成されたメモリカード２１０２のディレクトリ２１０３に格納する。

これにより、図２４に示すように、メモリカード２１０２においては、暗号化コンテンツ２１０５が、メモリカード２１０２へのその書出時刻を表わす書出時刻情報２１１３とともに同じディレクトリ２１０３に対応付けられて格納された状態となる。

また、図２５は、図２３の処理手順によってメモリカード２１０２に格納された暗号化コンテンツ２１０５を携帯電話機２１０１によって読み込んで復号化する際の、暗号化/復号化プログラム２１０９とコンテンツ格納ディレクトリ判別プログラム２１１０との処理手順を示すフロー図である。

図２５に示すように、コンテンツ格納ディレクトリ判別プログラム２１１０

は、ステップＳＴ２４０１において、メモリカード２１０２内に暗号化コンテンツがあるか否かを調べる。ここで肯定結果が得られると、このことは、携帯電話機２１０１によってメモリカード２１０２に書き出された暗号化コンテンツ、すなわち携帯電話機２１０１によって利用可能な暗号化コンテンツ２１０５がメモリカード２１０２に格納されている可能性があることを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム２１１０は、ステップＳＴ２４０２に移って、暗号化コンテンツと同一ディレクトリにある書出時刻情報を取得する。

そして、コンテンツ格納ディレクトリ判別プログラム２１１０は、ステップＳＴ２４０３に移って、ステップＳＴ２４０２において取得した書出時刻情報が、携帯電話機２１０１のＲＡＭ２１１１に格納されている書出時刻情報２１１３と同一であるか否かを判断する。

ここで否定結果が得られると、このことは、このとき取得した書出時刻情報が、携帯電話機２１０１によってメモリカード２１０１に書き出されたものではないこと、すなわち、この書出時刻情報と同一のディレクトリに格納されている暗号化コンテンツが、携帯電話機２１０１によってメモリカード２１０２に書き出されたものではないことを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム２１１０は、上述のステップＳＴ２４０１に戻って、メモリカード２１０２に他の暗号化コンテンツが格納されているか否かを判断し、当該判断結果に基づいて上述の場合と同様の処理を行う。

これに対して、ステップＳＴ２４０３において肯定結果が得られると、このことは、このとき取得した書出時刻情報が、携帯電話機２１０１によってメモリカード２１０１に書き出された書出時刻情報２１１３であること、すなわち、この書出時刻情報２１１３と同一のディレクトリ２１０３に格納されている暗号化コンテンツ２１０５が、携帯電話機２１０１によってメモリカード２１０２に書き出されたものであることを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム２１１０は、ステップＳＴ２４０４に移って、

当該書出時刻情報２１１３を一覧情報に追加した後、上述のステップＳＴ２４０１に戻って、メモリカード２１０２に他の暗号化コンテンツが格納されているか否かを判断し、当該判断結果に基づいて上述の場合と同様の処理を行う。

そして、メモリカード２１０２に格納されている暗号化コンテンツ（書出時刻情報）のすべてについて、携帯電話機２１０１によって書き出されたものであるか否かの判断が完了すると、コンテンツ格納ディレクトリ判別プログラム２１１０は、ステップＳＴ２４０１において否定結果を得ることにより、ステップＳＴ２４０５に移って、上述のステップＳＴ２４０４において作成された一覧情報によって特定される暗号化コンテンツ２１０５に関する情報を液晶画面１１６に一覧表示する。

これにより、液晶画面１１６には、メモリカード２１０２に格納されている暗号化コンテンツのうち、携帯電話機２１０１によって利用可能な暗号化コンテンツ２１０５に関連する情報（書出時刻情報等）が一覧表示される。

因みに、携帯電話機２１０１によって利用可能な暗号化コンテンツ２１０５に関する情報を一覧表示する構成としては、暗号化コンテンツ２１０５をメモリカード２１０２に格納する際に、その暗号化コンテンツ２１０５に対応したタイトル等の簡易情報のみを携帯電話機２１０１のＲＡＭ２１１１に格納し、ステップＳＴ２４０３における一致結果に基づいて、当該格納されている簡易情報を一覧表示する等の方法も考えられる。

ステップＳＴ２４０５において、液晶画面１１６にコンテンツの一覧が表示されると、利用者は、入力インターフェイス１１７を操作することにより、当該表示された一覧のなかから所望とするコンテンツを選択する。

これにより、暗号化/復号化プログラム２１０９は、ステップＳＴ２４０６に移って、メモリ読込プログラム１０８を用いて、このとき入力インターフェイス１１７を介して指定された暗号化コンテンツ２１０５をメモリカード２１０２から読み込み、さらに続くステップＳＴ２４０７に移って、ステップＳＴ２４０６においてメモリカード２１０２から取得した暗号化コンテンツ２１

０５を、ＲＯＭ２１１４に格納されている端末識別子２１１５を用いて復号化し、ＲＡＭ２１１１に格納する。

ＲＡＭ２１１１に格納されたコンテンツ２１１２は、携帯電話機２１０１の利用者が入力インターフェイス１１７を操作することにより起動され、利用者の利用に供される。

以上の構成において、携帯電話機２１０１は、メモリカード２１０２に暗号化コンテンツ２１０５を書き出す際に、その書出し時刻を時刻特定プログラム２１１９によってＲＡＭ２１１１に格納する。これにより、携帯電話機２１０１においては、当該携帯電話機２１０１においてのみ使用可能な暗号化コンテンツ２１０５を識別するための情報である書出時刻情報２１１３が、自身の環境に設定された状態となる。

そして、この設定された書出時刻情報２１１１は、暗号化コンテンツ２１０５とともにメモリカード２１０２の同じディレクトリ２１０３に格納される。これにより、暗号化コンテンツ２１０５と当該暗号化コンテンツ２１０５の利用環境（利用可能な携帯電話機２１０１）を識別するための書出時刻情報２１１３とが対応付けられてメモリカード２１０２に格納された状態となる。

このように、暗号化コンテンツ２１０５をメモリカード２１０２に書き出す際の書出時刻情報２１１３は、携帯電話機２１０１が暗号化コンテンツ２１０５をメモリカード２１０２に書き出したことの事実を表わすキーワードとして携帯電話機２１０１及びメモリカード２１０２の双方に格納される。

従って、携帯電話機２１０１に装着されたメモリカード２１０２に、当該携帯電話機２１０１に格納されている書出時刻情報２１１３と同一の時刻情報が格納されている場合には、当該書出時刻情報２１１３に対応付けられてメモリカード２１０２に格納されている暗号化コンテンツ２１０５は、携帯電話機２１０１によって書き出されたもの、すなわち、携帯電話機２１０１によって利用が可能なコンテンツであることを意味する。

従って、メモリカード２１０２に暗号化コンテンツ２１０５に対応付けられ

た格納されている書出時刻情報２１１３と、携帯電話機２１０１に格納されている書出時刻情報２１１３とが一致した場合、この書出時刻情報２１１３に対応付けられてメモリカード２１０２に格納されている暗号化コンテンツ２１０５は、携帯電話機２１０１に読み込んで、当該携帯電話機２１０１によって利用することが可能であり、この一致結果を受けて、携帯電話機２１０１の暗号化/復号化プログラム２１０９は、メモリカード２１０２から暗号化コンテンツ２１０５を読み込み、当該読み込まれた暗号化コンテンツ２１０５を復号化する。

このように、メモリカード２１０２の書出時刻情報２１１３が、ＲＡＭ２１１１に格納されている書出時刻情報２１１３と一致することを条件に、当該書出時刻情報２１１３に対応付けられた暗号化コンテンツ２１０５をメモリカード２１０２から携帯電話機２１０１に読み込んで復号化することにより、携帯電話機２１０１は、当該携帯電話機２１０１において利用可能である暗号化コンテンツ２１０５のみを、データ量の少ない書出時刻情報２１１３に基づいて選択することができる。

従って、メモリカード２１０２に複数の暗号化コンテンツが格納されている状態であって、これら複数の暗号化コンテンツを利用可能な端末装置（携帯電話機等）が各暗号化コンテンツ毎に異なる場合であっても、携帯電話機２１０１は、これら複数のデータ量の多い暗号化コンテンツをすべて復号化する必要はなく、当該複数の暗号化コンテンツにそれぞれ対応付けられた、データ量の少ない書出時刻情報２１１３を取得するだけで、利用可能な暗号化コンテンツ２１０５を判別することができる。

このように、本実施の形態のコンテンツ処理装置としての携帯電話機２１０１によれば、コンテンツ蓄積媒体であるメモリカード２１０２に格納された複数の暗号化コンテンツの判別を一段と容易に行うことが可能となり、携帯電話機２１０１において利用可能な暗号化コンテンツ２１０５を一段と迅速に復号化することができる。

なお、この実施の形態においては、暗号化コンテンツ２１０５を判別するための情報として、当該暗号化コンテンツ２１０５をメモリカード２１０２に書き出した書出時刻情報２１１３を用いる場合について述べたが、これに限らず、利用者が自ら入力インターフェイス１１７を操作して入力した設定情報、または携帯電話機２１０１が乱数等を用いてランダムに設定した値等を用いるようにしてもよい。また、これらの情報は、上述の書出時刻情報２１１３の場合を含めて、暗号化してメモリカード２１０２に格納するようにしてもよい。このようにすれば、書出時刻情報２１１３または、その他の暗号化コンテンツ２１０５を判別するための情報（利用者が設定した設定情報、携帯電話機２１０１がランダムに設定した値）が、メモリカード２１０２から第三者に知られた場合であっても、暗号化コンテンツ２１０５が不正に復号化されることを防止することができる。また、さらに書出時刻情報２１１３を予め設定されている識別子、または利用者が設定した識別子を用いて暗号化した後にメモリカード２１０２に格納するようにしてもよい。

また、この実施の形態においては、書出時刻情報２１１３をそのまま、メモリカード２１０２に格納する場合について述べたが、これに限らず、書出時刻情報２１１３を所定の変換式によって変換したものを格納するとともに、当該格納されたものを携帯電話機２１０１に読み込んでこれを逆変換式によって逆変換し、ＲＡＭ２１１１の書出時刻情報２１１３と比較するようにしてもよい。この場合、変換式としては、書出時刻情報２１１３の特定の位置（例えば下４桁）を抜き出したり、または、書出時刻情報２１１３の文字列を並び替える等、種々の変換式を用いることができる。

また、この実施の形態においては、書出時刻情報２１１３を暗号化コンテンツ２１０５と同じディレクトリ２１０３に格納する場合について述べたが、これに限らず、携帯電話機２１０１との間で認証を行うことによりアクセスが可能となる認証領域をメモリカード２１０２に設け、書出時刻情報２１１３を当該認証領域に格納するとともに、当該認証領域の書出時刻情報２１１３と通常

領域の暗号化コンテンツ２１０５との関係を表わすリンク情報を暗号化コンテンツ２１０５と同じディレクトリに格納するようにしてもよい。このようにすれば、メモリカード２１０２との間で認証に成功した携帯電話機２１０１のみが書出時刻情報２１１３を取得することができる。

また、この実施の形態の携帯電話機２１０１においては、端末識別子２１１５として、その携帯電話機２１０１の電話番号を用いる場合について述べたが、これに限らず、例えば携帯電話機２１０１の製造番号のようなその携帯電話機２１０１を識別するための識別子、又は、その他の何らかの意味を持つ文字列、数値、画像または音声等のデータ、若しくは特定のサービスと契約したことを示す識別子（会員番号等）を用いるようにしてもよい。また、この端末識別子２１１５として電話番号、製造番号、又はその他の文字列等の情報そのものではなく、端末識別子に対してある変換を加えた結果（端末識別子に関連する情報）を用いるようにしてもよい。このようにすれば、端末識別子によってコンテンツ及び特定データを暗号化する際の暗号化方法、及び端末識別子が第三者に漏洩した場合であっても、その端末識別子は、暗号化鍵となり得る他のデータに変換されていることにより、このデータ（暗号化鍵）によって暗号化された暗号化コンテンツ及び暗号化特定データが解読されることを防止することができる。

また、この実施の形態においては、コンテンツを格納するコンテンツ蓄積媒体としてメモリカード２１０２を用いる場合について述べたが、これに限らず、要はデジタル情報化されたコンテンツを格納可能なコンテンツ蓄積媒体であれば、他のデバイスを広く適用することができる。

（実施の形態７）

図２６は、本発明の実施の形態７に係るコンテンツ処理装置としての携帯電話機２５０１の構成を示すブロック図である。但し、図１及び図２と同一の構成となるものについては、図１及び図２と同一番号を付し、詳しい説明を省略する。

この図２６に示される携帯電話機２５０１は、ＲＡＭ２５１１に格納されているコンテンツ２５１２をメモリカード２５０２に書き出す際に、図２について上述した特定データ１１５に代えて、そのメモリカード２５０２におけるディレクトリ名２５１３を暗号化コンテンツ２５０５に対応付けて設定する点が図２の構成の携帯電話機１０１と異なる。

図２との対応部分に同一符号を付して示す図２６は、携帯電話機２５０１の構成を示すブロック図である。この図２６は、携帯電話機２５０１の構成のうち、特にコンテンツ処理に関わる構成を抽出して示すものである。携帯電話機２５０１は、それぞれ図示しないＣＰＵ（Central Processing Unit）によって動作するメモリ書出プログラム１０７、メモリ読込プログラム１０８、暗号化/復号化プログラム２５０９及びコンテンツ格納ディレクトリ判別プログラム２５１０を含んでいる。

図２６において、携帯電話機２５０１は、コンテンツプロバイダから携帯電話回線網を介してダウンロードしたコンテンツ２５１２をＲＡＭ（Random Access Memory）２５１１に格納する。暗号化/復号化プログラム２５０９は、ＲＡＭ２５１１に格納されたコンテンツ２５１２を暗号化するものであり、当該暗号化/復号化プログラム２５０９によって暗号化されたコンテンツ２５１２は、暗号化コンテンツ２５０５として、メモリ書出プログラム１０７によってメモリカードインターフェイス１０６を介してメモリカード２５０２に書き込まれる。

ＲＯＭ（Read Only Memory）２５１４は、携帯電話機２５０１に固有の所定の文字列（電話番号等）でなる識別子であって、コンテンツ２５１２を暗号化する際に用いられる端末識別子２５１５を格納している。

【０４０５】

暗号化/復号化プログラム２５０９は、コンテンツ２５１２を暗号化する際、ＲＯＭ（Read Only Memory）２５１４に格納されている端末識別子２５１５を用いて暗号化する。また、暗号化/復号化プログラム２５０９は、当該暗号化

されたコンテンツ２５１２（暗号化コンテンツ２５０５）をメモリカード２５０２に格納する際、当該格納先であるディレクトリ２５０３を作成し、当該ディレクトリ２５０３に暗号化コンテンツ２５０５を格納する。この携帯電話機２５０１によって作成されたディレクトリ２５０３のディレクトリ名２５１３は、当該携帯電話機２５０１のＲＡＭ２５１１にも格納される。

これにより、メモリカード２５０２に書き出された暗号化コンテンツのうち、携帯電話機２５０１によって書き出された暗号化コンテンツ２５０５は、そのディレクトリ名２５１３によって、携帯電話機２５０１において判別することができる状態となる。

また、メモリカード２５０２の所定のディレクトリ２５０３に格納された暗号化コンテンツ２５０５を携帯電話機２５０１に読み込む場合、携帯電話機２５０１のメモリ読込プログラム１０８は、暗号化コンテンツ２５０５を読み込む処理に先立って、携帯電話機２５０１のＲＡＭ２５１１に格納されているディレクトリ名２５１３と一致するディレクトリ名がメモリカード２５０２のディレクトリに存在するか否かを判断し、一致するディレクトリ名２５１３が存在する場合には、そのディレクトリを一覧情報化する。この一覧に載せられたディレクトリの暗号化コンテンツ２５０５は、携帯電話機２５０１によってメモリカード２５０２に書き出されたものであると判別することができる。

このように、メモリカード２５０２に設定されているディレクトリ２５０３が、携帯電話機２５０１によってメモリカード２５０２に設定されたものであることが判ると、暗号化/復号化プログラム２５０９は、当該ディレクトリ名２５１３がつけられたディレクトリ２５０３に格納されている暗号化コンテンツ２５０５を復号化し、当該復号化されたコンテンツ２５１２をＲＡＭ２５１１に格納する。

図２７は、携帯電話機２５０１のＲＡＭ２５１１に格納されているコンテンツ２５１２を、メモリカード２５０２に格納する際の、暗号化/復号化プログラム２５０９の処理手順を示すフロー図である。

図２７に示すように、暗号化/復号化プログラム２５０９は、ステップＳＴ２６０１において、まず、コンテンツ格納用のディレクトリ２５０３を作成した後、続くステップＳＴ２６０２に移って、ＲＡＭ２５１１からコンテンツ２５１２を取得する。そして、暗号化/復号化プログラム２５０９は、ステップＳＴ２６０３に移って、ステップＳＴ２６０２において取得したコンテンツ２５１２を、ＲＯＭ２５１４内の端末識別子２５１５を用いて例えばトリプルＤＥＳ暗号方式で暗号化する。

そして、暗号化/復号化プログラム２５０９は、ステップＳＴ２６０４に移って、ステップＳＴ２６０３において暗号化された暗号化コンテンツ２５０５を、ステップＳＴ２６０１において作成された、メモリカード２５０２のディレクトリ２５０３に格納する。

このときステップＳＴ２６０１において作成された暗号化コンテンツ２５０５の格納先であるディレクトリ２５０３のディレクトリ名２５１３は、ステップＳＴ２６０５において、暗号化/復号化プログラム２５０９によって携帯電話機２５０１のＲＡＭ２５１１に格納される。

これにより、図２８に示すように、メモリカード２５０２においては、暗号化コンテンツ２５０５が、携帯電話機２５０１のＲＡＭ２５１１に格納されたディレクトリ名２５１３と同じディレクトリ名のディレクトリ２５０３に格納された状態となる。

また、図２９は、図２７の処理手順によってメモリカード２５０２に格納された暗号化コンテンツ２５０５を携帯電話機２５０１によって読み込んで復号化する際の、暗号化/復号化プログラム２５０９とコンテンツ格納ディレクトリ判別プログラム２５１０との処理手順を示すフロー図である。

図２９に示すように、コンテンツ格納ディレクトリ判別プログラム２５１０は、ステップＳＴ２８０１において、メモリカード２５０２内に暗号化コンテンツがあるか否かを調べる。ここで肯定結果が得られると、このことは、携帯電話機２５０１によってメモリカード２５０２に書き出された暗号化コンテ

ンツ、すなわち携帯電話機２５０１によって利用可能な暗号化コンテンツ２５０５がメモリカード２５０２に格納されている可能性があることを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム２５１０は、ステップＳＴ２８０２に移って、暗号化コンテンツが格納されているディレクトリ名を取得する。

そして、コンテンツ格納ディレクトリ判別プログラム２５１０は、ステップＳＴ２８０３に移って、ステップＳＴ２８０２において取得したディレクトリ名が、携帯電話機２５０１のＲＡＭ２５１１に格納されているディレクトリ名２５１３と同一であるか否かを判断する。

ここで否定結果が得られると、このことは、このとき取得したディレクトリ名が、携帯電話機２５０１によって作成されメモリカード２５０１に設定されたものではないこと、すなわち、このディレクトリ名が付けられたディレクトリに格納されている暗号化コンテンツが、携帯電話機２５０１によってメモリカード２５０２に書き出されたものではないことを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム２５１０は、上述のステップＳＴ２８０１に戻って、メモリカード２５０２に他の暗号化コンテンツが格納されているか否かを判断し、当該判断結果に基づいて上述の場合と同様の処理を行う。

これに対して、ステップＳＴ２８０３において肯定結果が得られると、このことは、このとき取得したディレクトリ名が、携帯電話機２５０１によって作成されメモリカード２５０１に設定されたディレクトリ名２５１３であること、すなわち、このディレクトリ名２５１３が付けられたディレクトリ２５０３に格納されている暗号化コンテンツ２５０５が、携帯電話機２５０１によってメモリカード２５０２に書き出されたものであることを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム２５１０は、ステップＳＴ２８０４に移って、当該ディレクトリ名２５１３を一覧情報に追加した後、上述のステップＳＴ２８０１に戻って、メモリカード２５０２に他の暗号化コン

テンツが格納されているか否かを判断し、当該判断結果に基づいて上述の場合と同様の処理を行う。

そして、メモリカード２５０２に格納されている暗号化コンテンツ（ディレクトリ名）のすべてについて、携帯電話機２５０１によって書き出されたものであるか否かの判断が完了すると、コンテンツ格納ディレクトリ判別プログラム２５１０は、ステップＳＴ２８０１において否定結果を得ることにより、ステップＳＴ２８０５に移って、上述のステップＳＴ２８０４において作成された一覧情報によって特定される暗号化コンテンツ２５０５に関する情報（ディレクトリ名等）を液晶画面１１６に一覧表示する。

これにより、液晶画面１１６には、メモリカード２５０２に格納されている暗号化コンテンツのうち、携帯電話機２５０１によって利用可能な暗号化コンテンツ２５０５に関連する情報が一覧表示される。

因みに、携帯電話機２５０１によって利用可能な暗号化コンテンツ２５０５に関する情報を一覧表示する構成としては、暗号化コンテンツ２５０５をメモリカード２５０２に格納する際に、その暗号化コンテンツ２５０５に対応したタイトル等の簡易情報のみを携帯電話機２５０１のＲＡＭ２５１１に格納し、ステップＳＴ２８０３における一致結果に基づいて、当該格納されている簡易情報を一覧表示する等の方法も考えられる。

ステップＳＴ２８０５において、液晶画面１１６にコンテンツの一覧が表示されると、利用者は、入力インターフェイス１１７を操作することにより、当該表示された一覧のなかから所望とするコンテンツを選択する。

これにより、暗号化/復号化プログラム２５０９は、ステップＳＴ２８０６に移って、メモリ読込プログラム１０８を用いて、このとき入力インターフェイス１１７を介して指定された暗号化コンテンツ２５０５をメモリカード２５０２から読み込み、さらに続くステップＳＴ２８０７に移って、ステップＳＴ２８０６においてメモリカード２５０２から取得した暗号化コンテンツ２５０５を、ＲＯＭ２５１４に格納されている端末識別子２５１５を用いて復号化

し、ＲＡＭ２５１１に格納する。

ＲＡＭ２５１１に格納されたコンテンツ２５１２は、携帯電話機２５０１の利用者が入力インターフェイス１１７を操作することにより起動され、利用者の利用に供される。

以上の構成において、携帯電話機２５０１は、メモリカード２５０２に暗号化コンテンツ２５０５を書き出す際に、そのメモリカード２５０２での格納先であるディレクトリ２５０３のディレクトリ名２５１３をＲＡＭ２５１３に格納しておく。これにより、携帯電話機２５０１においては、当該携帯電話機２５０１においてのみ使用可能な暗号化コンテンツ２５０５が格納されたディレクトリ２５０３のディレクトリ名２５１３が、自身の環境に設定された状態となる。

そして、この設定されたディレクトリ名２５１３が付けられた、メモリカード２５０２のディレクトリ２５０３に、暗号化コンテンツ２５０５が格納される。これにより、ディレクトリ名２５１３は、暗号化コンテンツ２５０５の利用環境（利用可能な携帯電話機２５０１）を識別するための情報として利用可能な状態となる。

このように、暗号化コンテンツ２５０５をメモリカード２５０２に書き出す際のディレクトリ名２５１３は、携帯電話機２５０１が暗号化コンテンツ２５０５をメモリカード２５０２に書き出したことの事実を表わすキーワードとして携帯電話機２５０１及びメモリカード２５０２の双方に格納される。

従って、携帯電話機２５０１に装着されたメモリカード２５０２に、当該携帯電話機２５０１に格納されているディレクトリ名２５１３と同一のディレクトリ名が設定されている場合には、当該ディレクトリ名２５１３が付けられたディレクトリ２５０３に格納されている暗号化コンテンツ２５０５は、携帯電話機２５０１によって書き出されたもの、すなわち、携帯電話機２５０１によって利用が可能なコンテンツであることを意味する。

従って、メモリカード２５０２のディレクトリ名と、携帯電話機２５０１に

格納されているディレクトリ名２５１３とが一致した場合、このディレクトリ名２５１３が付けられた、メモリカード２５０２のディレクトリ２５０３に格納されている暗号化コンテンツ２５０５は、携帯電話機２５０１に読み込んで、当該携帯電話機２５０１によって利用することが可能であり、この一致結果を受けて、携帯電話機２５０１の暗号化/復号化プログラム２５０９は、メモリカード２５０２から当該暗号化コンテンツ２５０５を読み込み、当該読み込まれた暗号化コンテンツ２５０５を復号化する。

このように、メモリカード２５０２のディレクトリ名が、ＲＡＭ２５１１に格納されているディレクトリ名２５１３と一致することを条件に、当該ディレクトリ名２５１３が付けられた、メモリカード２５０２のディレクトリ２５０３に格納されている暗号化コンテンツ２５０５をメモリカード２５０２から携帯電話機２５０１に読み込んで復号化することにより、携帯電話機２５０１は、当該携帯電話機２５０１において利用可能である暗号化コンテンツ２５０５のみを、データ量の少ないディレクトリ名２１１３に基づいて選択することができる。

従って、メモリカード２５０２に複数の暗号化コンテンツが格納されている状態であって、これら複数の暗号化コンテンツを利用可能な端末装置（携帯電話機等）が各暗号化コンテンツ毎に異なる場合であっても、携帯電話機２５０１は、これら複数のデータ量の多い暗号化コンテンツをすべて復号化する必要はなく、当該複数の暗号化コンテンツにそれぞれ対応付けられた、データ量の少ないディレクトリ名２５１３を取得するだけで、利用可能な暗号化コンテンツ２５０５を判別することができる。

このように、本実施の形態のコンテンツ処理装置としての携帯電話機２５０１によれば、コンテンツ蓄積媒体であるメモリカード２５０２に格納された複数の暗号化コンテンツの判別を一段と容易に行うことが可能となり、携帯電話機２５０１において利用可能な暗号化コンテンツ２５０５を一段と迅速に復号化することができる。

なお、この実施の形態においては、暗号化コンテンツ２５０５を判別するための情報として、当該暗号化コンテンツ２５０５をメモリカード２５０２に書き出す際のディレクトリ名２５１３を携帯電話機２５０１において自動的に作成する場合について述べたが、これに限らず、利用者が自ら入力インターフェイス１１７を操作して入力した設定情報、または携帯電話機２５０１が乱数等を用いてランダムに設定した値等を用いるようにしてもよい。また、このようにして作成されたディレクトリ名２５１３は、上述の実施の形態のディレクトリ名２５１３の場合を含めて、暗号化してメモリカード２５０２のディレクトリ名として設定するようにしてもよい。このようにすれば、暗号化コンテンツ２５０５を判別するための、携帯電話機２５０１によって作成されたディレクトリ名が、メモリカード２５０２から第三者に知られた場合であっても、暗号化コンテンツ２５０５が不正に復号化されることを防止することができる。

また、この実施の形態の携帯電話機２５０１においては、端末識別子２５１５として、その携帯電話機２５０１の電話番号を用いる場合について述べたが、これに限らず、例えば携帯電話機２５０１の製造番号のようなその携帯電話機２５０１を識別するための識別子、又は、その他の何らかの意味を持つ文字列、数値、画像または音声等のデータ、若しくは特定のサービスと契約したことを示す識別子（会員番号等）を用いるようにしてもよい。また、この端末識別子２５１５として電話番号、製造番号、又はその他の文字列等の情報そのものではなく、端末識別子に対してある変換を加えた結果（端末識別子に関連する情報）を用いるようにしてもよい。このようにすれば、端末識別子によってコンテンツ及び特定データを暗号化する際の暗号化方法、及び端末識別子が第三者に漏洩した場合であっても、その端末識別子は、暗号化鍵となり得る他のデータに変換されていることにより、このデータ（暗号化鍵）によって暗号化された暗号化コンテンツ及び暗号化特定データが解読されることを防止することができる。

また、この実施の形態においては、携帯電話機２５０１のＲＡＭ２５１１に、

メモリカード２５０２のディレクトリ名２５１３を格納し、当該携帯電話機１５０１によって利用可能な暗号化コンテンツ２５０５を、当該ディレクトリ名２５１３によって判別する場合について述べたが、これに限らず、メモリカード２５０２に固有のカード識別子を、携帯電話機２５０１のＲＡＭ２５１１とメモリカード２５０２の双方によって共有し、当該カード識別子及びそのディレクトリ名２５１３の両方によって、利用可能な暗号化コンテンツ２５０５を判別するようにしてもよい。このようにすれば、複数のメモリカードをコンテンツの種類（オーディオ用、ゲーム用、等）ごとに使い分ける場合に対応することができる。また、このようにすれば、同じディレクトリ名を有する異なるメモリカードについても、これらのメモリカードに格納されている各暗号化コンテンツを利用可能であるか否かを判別することができる。

また、この実施の形態においては、コンテンツを格納するコンテンツ蓄積媒体としてメモリカード２５０２を用いる場合について述べたが、これに限らず、要はデジタル情報化されたコンテンツを格納可能なコンテンツ蓄積媒体であれば、他のデバイスを広く適用することができる。

（実施の形態８）

上述の実施の形態１～実施の形態７においては、１つの携帯電話機において、メモリカードに格納されている複数の暗号化コンテンツのなかから自身で利用可能なコンテンツを判別する場合について述べたが、本発明はこれに限らず、１つのメモリカードを異なる携帯電話機に差し替えて、これら複数の携帯電話機において当該１つのメモリカードを利用する場合においても、適用することができる。

この場合、携帯電話機のＲＯＭに格納される端末識別子として、１つのメモリカードの利用を共有する複数の携帯電話機において共通の端末識別子を格納しておく。このようにすれば、特定の識別子を持つ環境を複数の携帯電話機に設定することができ、１つのメモリカードを複数の携帯電話機を含む環境で利用することが可能となる。

以上説明したように、本発明によれば、コンテンツ蓄積媒体に格納された暗号化コンテンツについて、当該暗号化コンテンツに関連したデータ量の少ない情報を当該暗号化コンテンツに対応付けてコンテンツ蓄積媒体に格納することにより、データ量の多い暗号化コンテンツを復号化することなく、関連した情報に基づいて暗号化コンテンツを容易に判別することができる。

また、本発明によれば、コンテンツ蓄積媒体に格納されているコンテンツが使用可能であるか否かを判断することが可能となることにより、正規のデータでないデータを誤って再生してしまうといった不都合を防止することができる。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報の前記コンテンツ蓄積媒体への書き込みを行うコンテンツ処理装置であって、前記識別子又は前記識別子に関連する情報を暗号化の鍵として特定のデータを暗号化するデータ暗号化部と、前記暗号化された特定のデータを前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化データ格納部と、を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記暗号化データ格納部は、前記暗号化された特定のデータの前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納するとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された特定のデータとの関連付けを行なう構成を採る。

この構成によれば、コンテンツ蓄積媒体の認証領域にアクセス可能な場合にのみ暗号化コンテンツの判別を行うことができる。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用

を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報の前記コンテンツ蓄積媒体への書き込みを行うコンテンツ処理装置であって、前記識別子を前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する識別子格納部、を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記識別子格納部は、前記識別子の前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納するとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された識別子との関連付けを行なう構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記蓄積媒体に書き込むコンテンツ処理装置であって、特定の暗号化手段を用いて前記識別子を暗号化する識別子暗号化部と、前記暗号化された識別子を前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化識別子格納部と、を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記暗号化識別子格納部は、前記暗号化識別子の前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納し、同時に前記デジタル情報のファイルと前記認証ファイルシステム内に格納された暗号化識別子との関連付けを行なう構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記コンテンツ処理装置は、さらに、前記識別子を特定の変換式に対応して変換する識別子変換部を具備し、前記識別子暗号化部は、前記識別子変換部によって変換された識別子を暗号化し、前記暗号化識別子格納部は、当該暗号化された識別子を前記コン

テンツ蓄積媒体に格納する構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理装置であって、前記識別子とは異なる、前記特定の識別子を持つ環境に固有な特定のデータを、前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する固有データ格納部を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記固有データ格納部は、前記特定のデータの前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納するとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された前記特定のデータとの関連付けを行なう構成を採る。

本発明のコンテンツ処理装置は、デジタル情報を着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理装置であって、前記デジタル情報を前記コンテンツ蓄積媒体に書き込んだ時刻を特定する書き込み時刻特定部と、前記特定された時刻を、書き込みを行なう自身の環境に格納するとともに、前記デジタル情報のファイルと関連付けた上で前記コンテンツ蓄積媒体に格納する書き込み時刻格納部とを具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記書き込み時刻格納部は、前記書き込み時刻の前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納するとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された前

記書き込み時刻との関連付けを行なう構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記コンテンツ処理装置は、さらに、前記書き込み時刻を前記識別子に関連する情報を用いて暗号化する書き込み時刻暗号化部を備え、前記書き込み時刻格納部は、少なくともコンテンツ蓄積媒体に格納する書き込み時刻を、前記書き込み時刻暗号化部によって暗号化されたものとする構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記コンテンツ処理装置は、さらに、前記識別子に関連する情報を利用して前記書き込み時刻を変換する書き込み時刻変換部を具備し、前記書き込み時刻暗号化部は、前記変換された書き込み時刻を特定の方法で暗号化する構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理装置であって、ユーザが指定する値あるいは名称であるユーザ指定値を環境に設定するユーザ指定値書き込み部と、前記ユーザ指定値を前記コンテンツ蓄積媒体に格納するユーザ指定値格納部とを備える構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記コンテンツ処理装置は、さらに、ユーザがユーザ指定値を指定していない状態でユーザ指定値として利用するための初期値をランダムに設定する、初期値設定部を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記コンテンツ処理装置は、さらに、前記ユーザ指定値を前記識別子に関連する情報を用いて暗号化するユーザ指定値暗号化部を具備し、前記ユーザ指定値格納部は、前記コンテンツ蓄積媒体に格納するユーザ指定値を、前記

ユーザ指定値暗号化部によって暗号化されたものとする構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理装置であって、前記デジタル情報を前記コンテンツ蓄積媒体に書き込む際に特定のデータを作成する書き込み特定データ生成部と、前記特定のデータを、書き込みを行なう自身の環境に格納するとともに、前記デジタル情報のファイルと関連付けた上で前記コンテンツ蓄積媒体に格納する書き込み特定データ格納部と、を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記書き込み特定データ生成部において、前記特定のデータは、書き込みの際にランダムに生成されるか、あるいは特定の手順によって生成される構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理装置であって、前記デジタル情報を前記コンテンツ蓄積媒体に書き込んだ際の書き込み箇所を特定する書き込み箇所特定部と、前記特定された箇所を、書き込みを行なう自身の環境に格納する書き込み箇所格納部と、を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記デジタル情報は、前記識別子に関連する情報を利用して暗号化されている構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記特定のデータは、なんらかの意味を持つ文字列、数値、画像、音声等のデータである構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記識別子は、なんらかの意味を持つ文字列、数値、画像、音声等のデータである構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記特定の環境または

特定の識別子を持つ環境は、前記着脱可能なコンテンツ蓄積媒体を着脱することのできる特定の機器である構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記特定の環境または特定の識別子を持つ環境は、特定のサービスと契約したことを示す識別子によって特定される環境である構成を採る。

以上の構成によれば、コンテンツ蓄積媒体に格納された複数の暗号化コンテンツの判別を、当該暗号化コンテンツに関連付けられた情報に基づいて、一段と容易に行うようにすることができる。また、コンテンツ蓄積媒体に格納されているコンテンツが使用可能であるか否かを判断することが可能となり、正規のデータでないデータを誤って再生してしまうといった不都合を防止することができる。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された暗号化データを読み出す暗号化データ読み出し部と、前記読み出された暗号化データを自身の環境の識別子に関連する情報によって復号化し、特定のデータと合致するかどうかを判定する暗号化データ判別部と、を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記暗号化データ読み出し部は、前記暗号化された特定のデータを、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出す構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用

を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された識別子を読み出し、自身の環境の識別子と合致するかどうかを判定する識別子判別部、を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記識別子判別部は、前記識別子を、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出す構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された暗号化識別子を読み出す暗号化識別子読み出し部と、前記読み出された暗号化識別子を自身の環境の特定の復号化手段によって復号化し、自身の識別子と合致するかどうかを判定する暗号化識別子判別部と、を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記暗号化識別子読み出し部は、前記暗号化識別子を、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出す構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記コンテンツ処理装置は、さらに、前記暗号化識別子を特定の変換式に対応して変換する識別子逆変換部を具備し、前記暗号化識別子判別部は、復号化した暗号化識別子を前記識別子逆変換部で逆変換してから自身の識別子と合致するかどうかを判定す

る構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された固有データを読み出す固有データ読み出し部と、前記読み出された固有データを自身の環境の固有データと合致するかどうかを判定する固有データ判別部と、を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記固有データ読み出し部は、前記固有データを、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出す構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルと関連付けられた前記デジタル情報の書き込み時刻を読み出す書き込み時刻読み出し部と、前記読み出された書き込み時刻と、自身の環境に格納されている書き込み時刻のひとつとが合致するか否かを判定する書き込み時刻判別部と、を具備する構成を採る。

本発明のコンテンツ処理装置は、前記書き込み時刻読み出し部は、前記書き込み時刻を、前記着脱可能なコンテンツ蓄積媒体と前記特定の環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出す構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記書き込み時刻判別部は、前記書き込み時刻読み出し部で読み出された書き込み時刻を、自身の環境の持つ識別子に関連する情報を用いて復号してから自身の環境に格納されている書き込み時刻のひとつと合致するか否かを判定する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記コンテンツ処理装置は、さらに、前記書き込み時刻読み出し部で読み出された書き込み時刻を、前記識別子に関連する情報を利用して変換する書き込み時刻変換部を具備し、前記書き込み時刻判別部は、前記変換された書き込み時刻を特定の方法で復号してから自身の環境に格納されている書き込み時刻のひとつと合致するか否かを判定する構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルと関連付けられた、ユーザによって指定されたユーザ指定値を読み出すユーザ指定値読み出し部と、前記読み出されたユーザ指定値と、自身の環境に格納されているユーザ指定値が合致するか否かを判定するユーザ指定値判別部と、を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記ユーザ指定値判別部は、前記ユーザ指定値読み出し部で読み出されたユーザ指定値を、自身の環境の持つ識別子に関連する情報を用いて復号してから自身の環境に格納されているユーザ指定値と合致するか否かを判定する構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルと関連付けられた特定のデータを読み出す書き込み特定データ読み出し部と、前記読み出された特定のデータと、自身の環境に格納されている特定のデータのひとつと合致するか否かを判定する書き込み特定データ判別部と、を具備する構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルの格納箇所である書き込み箇所を前記コンテンツ蓄積媒体上から読み出す書き込み箇所読み出し部と、前記読み出された書き込み箇所と、自身の環境に格納されている書き込み箇所のひとつと合致するか否かを判定する書き込み箇所判別部と、を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記特定の環境または特定の識別子を持つ環境は、前記着脱可能なコンテンツ蓄積媒体を着脱することのできる特定の機器である構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記特定の環境または特定の識別子を持つ環境は、特定のサービスと契約したことを示す識別子によって特定される環境である構成を採る。

以上の構成によれば、コンテンツ蓄積媒体に格納された暗号化コンテンツを読み出し、復号化する前に、当該暗号化コンテンツに関連付けられた情報を基に、暗号化コンテンツを判別することにより、暗号化コンテンツを復号化することなく、その内容を容易に判別することができる。また、コンテンツ蓄積媒

体に格納されているコンテンツが使用可能であるか否かを判断することが可能となり、正規のデータでないデータを誤って再生してしまうといった不都合を防止することができる。

本発明のコンテンツ蓄積媒体は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体であって、前記識別子又は前記識別子に関連する情報を暗号化の鍵として暗号化された特定のデータが、前記デジタル情報のファイルと関連付けられて格納されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記コンテンツ蓄積媒体は、さらに、前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステムを具備し、前記暗号化された特定のデータは、前記認証ファイルシステム内に格納されているとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された特定のデータとの関連付けが記録されている構成を採る。

本発明のコンテンツ蓄積媒体は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体であって、前記識別子が前記デジタル情報のファイルと関連付けて格納されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記コンテンツ蓄積媒体は、さらに、前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステムを具備し、前記識別子は、前記認証ファイルシステム内に格納されているとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された識別子との関連付けが記録されている構成を採る。

本発明のコンテンツ蓄積媒体は、デジタル情報化されたコンテンツを着脱可

能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体であって、特定の暗号化手段を用いて暗号化された前記識別子が、前記デジタル情報のファイルと関連付けて格納されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記コンテンツ蓄積媒体は、さらに、前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステムを具備し、前記暗号化識別子は、前記認証ファイルシステム内に格納されているとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された暗号化識別子との関連付けが記録されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記識別子は、特定の変換式に対応して変換された上で前記特定の暗号化手段を用いて暗号化されている構成を採る。

本発明のコンテンツ蓄積媒体は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体であって、前記識別子とは異なる、前記特定の識別子を持つ環境に固有な特定のデータが、前記デジタル情報のファイルと関連付けられて格納されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記コンテンツ蓄積媒体は、さらに、前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステムを具備し、前記固有の特定データは、前記認証ファイルシステム内に格納されているとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された前記固有の特定データとの関連付けが記録されている構成を採る。

本発明のコンテンツ蓄積媒体は、デジタル情報化されたコンテンツを着脱可

能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体であって、前記デジタル情報が書き込まれた時刻を特定する書き込み時刻が、前記デジタル情報のファイルと関連付けられた上で格納されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記コンテンツ蓄積媒体は、さらに、前記特定の環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステムを具備し、前記書き込み時刻は、前記認証ファイルシステム内に格納されているとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された前記書き込み時刻との関連付けが記録されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記書き込み時刻は前記識別子に関連する情報を用いて暗号化されて格納されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記書き込み時刻は、前記識別子に関連する情報を利用して変換されたのち、特定の方法で暗号化されている構成を採る。

本発明のコンテンツ蓄積媒体は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体であって、ユーザが環境に対して指定する値あるいは名称であるユーザ指定値が、前記デジタル情報のファイルと関連付けられた上で格納されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記ユーザ指定値としては、ユーザがユーザ指定値を指定していない状態では、初期値としてランダムな値が格納されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記ユーザ指定値は前記識別子に関連する情報を用いて暗号化されて格納されている構成を採る。

本発明のコンテンツ蓄積媒体は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体であって、前記デジタル情報が書き込まれる際に生成された特定のデータが、前記デジタル情報のファイルと関連付けられた上で格納されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記特定のデータは、書き込みの際にランダムに生成されるか、あるいは特定の手順によって生成されて格納されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記デジタル情報は、前記識別子に関連する情報を利用して暗号化されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記特定のデータは、なんらかの意味を持つ文字列、数値、画像、音声等のデータである構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記識別子は、なんらかの意味を持つ文字列、数値、画像、音声等のデータである構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記識別子は、特定のサービスと契約したことを示すデータである構成を採る。

以上の構成によれば、コンテンツ蓄積媒体において、暗号化コンテンツに関連付けられた情報が格納されることにより、当該情報に基づいて、暗号化コンテンツの判別を一段と容易に行わせることができる。また、この情報によって、コンテンツ蓄積媒体に格納されているコンテンツが使用可能であるか否かを端末装置等の使用環境に判断させることが可能となり、当該使用環境が正規のデータでないデータを誤って再生してしまうといった不都合を防止すること

ができる。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報の前記コンテンツ蓄積媒体への書き込みを行うコンテンツ処理方法であって、前記識別子に関連する情報を暗号化の鍵として特定のデータを暗号化するデータ暗号化ステップと、前記暗号化された特定のデータを前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化データ格納ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記暗号化データ格納ステップでは、前記暗号化された特定のデータの前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された特定のデータとの関連付けが行なわれるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報の前記コンテンツ蓄積媒体への書き込みを行うコンテンツ処理方法であって、前記識別子を前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する識別子格納ステップを具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記識別子格納ステップは、前記識別子の前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納

された識別子との関連付けが行なわれるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記蓄積媒体に書き込むコンテンツ処理方法であって、特定の暗号化手段を用いて前記識別子を暗号化する識別子暗号化ステップと、前記暗号化された識別子を前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化識別子格納ステップと、を備えるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記暗号化識別子格納ステップでは、前記暗号化識別子の前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された暗号化識別子との関連付けが行なわれるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記コンテンツ処理方法は、さらに、前記識別子を特定の変換式に対応して変換する識別子変換ステップを具備し、前記識別子暗号化ステップでは、前記識別子変換ステップによって変換された識別子が暗号化され、前記暗号化識別子格納ステップでは、当該暗号化された識別子が前記コンテンツ蓄積媒体に格納されるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理方法であって、前記識別子とは異なる、前記特定の識別子を持つ環境に固有な特定のデータを、前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する固有データ格納ステップを備えるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記固有データ格納ス

テップでは、前記特定のデータの前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された前記特定のデータとの関連付けが行なわれるようにした。

本発明のコンテンツ処理方法は、デジタル情報を着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理方法であって、前記デジタル情報を前記コンテンツ蓄積媒体に書き込んだ時刻を特定する書き込み時刻特定ステップと、前記特定された時刻を、書き込みを行なう自身の環境に格納するとともに、前記デジタル情報のファイルと関連付けた上で前記コンテンツ蓄積媒体に格納する書き込み時刻格納ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記書き込み時刻格納ステップでは、前記書き込み時刻の前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された前記書き込み時刻との関連付けが行なわれるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記コンテンツ処理方法は、さらに、前記書き込み時刻を前記識別子に関連する情報を用いて暗号化する書き込み時刻暗号化ステップを備え、前記書き込み時刻格納ステップでは、少なくともコンテンツ蓄積媒体に格納する書き込み時刻が、前記書き込み時刻暗号化部によって暗号化されたものとなるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記コンテンツ処理方

法は、さらに、前記識別子に関連する情報を利用して前記書き込み時刻を変換する書き込み時刻変換ステップを具備し、前記書き込み時刻暗号化ステップでは、前記変換された書き込み時刻が特定の方法で暗号化されるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理方法であって、ユーザが指定する値あるいは名称であるユーザ指定値を環境に設定するユーザ指定値書き込みステップと、前記ユーザ指定値を前記コンテンツ蓄積媒体に格納するユーザ指定値格納ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、さらに、ユーザがユーザ指定値を指定していない状態でユーザ指定値として利用するための初期値をランダムに設定する、初期値設定ステップを具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記コンテンツ処理方法は、さらに、前記ユーザ指定値を前記識別子に関連する情報を用いて暗号化するユーザ指定値暗号化ステップを具備し、前記ユーザ指定値格納ステップでは、前記コンテンツ蓄積媒体に格納するユーザ指定値が、前記ユーザ指定値暗号化部によって暗号化されたものとなるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理方法であって、前記デジタル情報を前記コンテンツ蓄積媒体に書き込む際に特定のデータを作成する書き込み特定データ生成ステップと、前記特定のデータを、書き込みを行なう自身の環境に格納するとともに、前記デジタル情報のファイルと関連付けた上で

前記コンテンツ蓄積媒体に格納する書き込み特定データ格納ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記書き込み特定データ生成ステップにおいて、前記特定のデータは、書き込みの際にランダムに生成されるか、あるいは特定の手順によって生成されるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理方法であって、前記デジタル情報を前記コンテンツ蓄積媒体に書き込んだ際の書き込み箇所を特定する書き込み箇所特定ステップと、前記特定された箇所を、書き込みを行なう自身の環境に格納する書き込み箇所格納ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記デジタル情報は、前記識別子に関連する情報を利用して暗号化されているようにした。

本発明のコンテンツ処理方法は、上記方法において、前記特定のデータは、なんらかの意味を持つ文字列、数値、画像、音声等のデータであるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記識別子は、なんらかの意味を持つ文字列、数値、画像、音声等のデータであるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記特定の環境または特定の識別子を持つ環境は、前記着脱可能なコンテンツ蓄積媒体を着脱することのできる特定の機器であるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記特定の環境または特定の識別子を持つ環境は、特定のサービスと契約したことを示す識別子によって特定される環境であるようにした。

以上の方法によれば、コンテンツ蓄積媒体に格納された複数の暗号化コンテンツの判別を、当該暗号化コンテンツに関連付けられた情報に基づいて、一段と容易に行うようにすることができる。また、コンテンツ蓄積媒体に格納され

ているコンテンツが使用可能であるか否かを判断することが可能となり、正規のデータでないデータを誤って再生してしまうといった不都合を防止することができる。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された暗号化データを読み出す暗号化データ読み出しステップと、前記読み出された暗号化データを自身の環境の識別子に関連する情報によって復号化し、特定のデータと合致するかどうかを判定する暗号化データ判別ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記暗号化データ読み出しステップでは、前記暗号化された特定のデータは、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出されるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された識別子を読み出し、自身の環境の識別子と合致するかどうかを判定する識別子判別ステップ、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記識別子判別ステップでは、前記識別子は、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前

記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出されるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された暗号化識別子を読み出す暗号化識別子読み出しステップと、前記読み出された暗号化識別子を自身の環境の特定の復号化手段によって復号化し、自身の識別子と合致するかどうかを判定する暗号化識別子判別ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記暗号化識別子読み出しステップでは、前記暗号化識別子は、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出されるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記コンテンツ処理方法は、さらに、前記暗号化識別子を特定の変換式に対応して変換する識別子逆変換ステップを具備し、前記暗号化識別子判別ステップでは、復号化された暗号化識別子は、前記識別子逆変換部で逆変換されてから自身の識別子と合致するか否かが判定されるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された固有データを読み出す固有データ読み出しステップと、

前記読み出された固有データを自身の環境の固有データと合致するかどうかを判定する固有データ判別ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記固有データ読み出しステップでは、前記固有データは、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出されるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルと関連付けられた前記デジタル情報の書き込み時刻を読み出す書き込み時刻読み出しステップと、前記読み出された書き込み時刻と、自身の環境に格納されている書き込み時刻のひとつとが合致するか否かを判定する書き込み時刻判別ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記書き込み時刻読み出しステップでは、前記書き込み時刻は、前記着脱可能なコンテンツ蓄積媒体と前記特定の環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出されるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記書き込み時刻判別ステップでは、前記書き込み時刻読み出しステップで読み出された書き込み時刻が、自身の環境の持つ識別子に関連する情報を用いて復号されてから自身の環境に格納されている書き込み時刻のひとつと合致するか否か判定されるようにした。

本発明のコンテンツ処理方法は、上記方法において、さらに、前記書き込み時刻読み出しステップで読み出された書き込み時刻を、前記識別子に関連する情報を利用して変換する書き込み時刻変換ステップを具備し、前記書き込み時刻判別ステップでは、前記変換された書き込み時刻が特定の方法で復号されてから自身の環境に格納されている書き込み時刻のひとつと合致するか否かが判定されるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルと関連付けられた、ユーザによって指定されたユーザ指定値を読み出すユーザ指定値読み出しステップと、前記読み出されたユーザ指定値と、自身の環境に格納されているユーザ指定値が合致するか否かを判定するユーザ指定値判別ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記ユーザ指定値判別ステップでは、前記ユーザ指定値読み出し部で読み出されたユーザ指定値は、自身の環境の持つ識別子に関連する情報を用いて復号されてから自身の環境に格納されているユーザ指定値と合致するか否か判定されるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルと関連付けられた特定のデータを読み出す書き込み特定データ読み出しステップと、前記読み

出された特定のデータと、自身の環境に格納されている特定のデータのひとつと合致するか否かを判定する書き込み特定データ判別ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルの格納箇所である書き込み箇所を前記コンテンツ蓄積媒体上から読み出す書き込み箇所読み出しステップと、前記読み出された書き込み箇所と、自身の環境に格納されている書き込み箇所のひとつと合致するか否かを判定する書き込み箇所判別ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記特定の環境または特定の識別子を持つ環境は、前記着脱可能なコンテンツ蓄積媒体を着脱することのできる特定の機器であるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記特定の環境または特定の識別子を持つ環境は、特定のサービスと契約したことを示す識別子によって特定される環境であるようにした。

以上の方法によれば、コンテンツ蓄積媒体に格納された暗号化コンテンツを読み出し、復号化する前に、当該暗号化コンテンツに関連付けられた情報を基に、暗号化コンテンツを判別することにより、暗号化コンテンツを復号化することなく、その内容を容易に判別することができる。また、コンテンツ蓄積媒体に格納されているコンテンツが使用可能であるか否かを判断することが可能となり、正規のデータでないデータを誤って再生してしまうといった不都合を防止することができる。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報

の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報の前記コンテンツ蓄積媒体への書き込みを行うコンテンツ処理プログラムであって、前記識別子に関連する情報を暗号化の鍵として特定のデータを暗号化するデータ暗号化ステップと、前記暗号化された特定のデータを前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化データ格納ステップと、を具備するようにした。

本発明のコンテンツ処理プログラムは、前記暗号化データ格納ステップでは、前記暗号化された特定のデータの前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された特定のデータとの関連付けが行なわれるようにした。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報の前記コンテンツ蓄積媒体への書き込みを行うコンテンツ処理プログラムであって、前記識別子を前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する識別子格納ステップを具備するようにした。

本発明のコンテンツ処理プログラムは、前記識別子格納ステップでは、前記識別子の前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された識別子との関連付けが行なわれるようにした。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報

の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記蓄積媒体に書き込むコンテンツ処理プログラムであって、特定の暗号化手段を用いて前記識別子を暗号化する識別子暗号化ステップと、前記暗号化された識別子を前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化識別子格納ステップと、を備えるようにした。

本発明のコンテンツ処理プログラムは、前記暗号化識別子格納ステップでは、前記暗号化識別子の前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された暗号化識別子との関連付けが行なわれるようにした。

本発明のコンテンツ処理プログラムは、前記コンテンツ処理方法は、さらに、前記識別子を特定の変換式に対応して変換する識別子変換ステップを具備し、前記識別子暗号化ステップでは、前記識別子変換ステップによって変換された識別子が暗号化され、前記暗号化識別子格納ステップでは、当該暗号化された識別子が前記コンテンツ蓄積媒体に格納されるようにした。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理プログラムであって、前記識別子とは異なる、前記特定の識別子を持つ環境に固有な特定のデータを、前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する固有データ格納ステップを備えるようにした。

本発明のコンテンツ処理プログラムは、前記固有データ格納ステップでは、前記特定のデータの前記コンテンツ蓄積媒体上の格納先として、前記着脱可能

なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された前記特定のデータとの関連付けが行なわれるようにした。

本発明のコンテンツ処理プログラムは、デジタル情報を着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムに用いられる、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理プログラムであって、前記デジタル情報を前記コンテンツ蓄積媒体に書き込んだ時刻を特定する書き込み時刻特定ステップと、前記特定された時刻を、書き込みを行なう自身の環境に格納するとともに、前記デジタル情報のファイルと関連付けた上で前記コンテンツ蓄積媒体に格納する書き込み時刻格納ステップと、を具備するようにした。

本発明のコンテンツ処理プログラムは、前記書き込み時刻格納ステップでは、前記書き込み時刻の前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された前記書き込み時刻との関連付けが行なわれるようにした。

本発明のコンテンツ処理プログラムは、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記コンテンツ処理プログラムは、さらに、前記書き込み時刻を前記識別子に関連する情報を用いて暗号化する書き込み時刻暗号化ステップを備え、前記書き込み時刻格納ステップでは、少なくともコンテンツ蓄積媒体に格納する書き込み時刻が、前記書き込み時刻暗号化部によって暗号化されたものとなるようにした。

本発明のコンテンツ処理プログラムは、さらに、前記識別子に関連する情報を利用して前記書き込み時刻を変換する書き込み時刻変換ステップを具備し、

前記書き込み時刻暗号化ステップでは、前記変換された書き込み時刻が特定の方法で暗号化されるようにした。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理プログラムであって、ユーザが指定する値あるいは名称であるユーザ指定値を環境に設定するユーザ指定値書き込みステップと、前記ユーザ指定値を前記コンテンツ蓄積媒体に格納するユーザ指定値格納ステップと、を具備するようにした。

本発明のコンテンツ処理プログラムは、さらに、ユーザがユーザ指定値を指定していない状態でユーザ指定値として利用するための初期値をランダムに設定する、初期値設定ステップを具備するようにした。

本発明のコンテンツ処理プログラムは、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記コンテンツ処理プログラムは、さらに、前記ユーザ指定値を前記識別子に関連する情報を用いて暗号化するユーザ指定値暗号化ステップを具備し、前記ユーザ指定値格納ステップでは、前記コンテンツ蓄積媒体に格納するユーザ指定値が、前記ユーザ指定値暗号化部によって暗号化されたものとなるようにした。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理プログラムであって、前記デジタル情報を前記コンテンツ蓄積媒体に書き込む際に特定のデータを作成する書き込み特定データ生成ステップと、前記特定のデータを、書き込みを行なう自身の環境に格納するとともに、前記デジタル情報のファイルと関連付けた上で前記コンテンツ蓄積媒体に格納する書き込み特定データ格納ステップと、を具備するようにした。

本発明のコンテンツ処理プログラムは、前記書き込み特定データ生成ステップにおいて、前記特定のデータは、書き込みの際にランダムに生成されるか、あるいは特定の手順によって生成されるようにした。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理プログラムであって、前記デジタル情報を前記コンテンツ蓄積媒体に書き込んだ際の書き込み箇所を特定する書き込み箇所特定ステップと、前記特定された箇所を、書き込みを行なう自身の環境に格納する書き込み箇所格納ステップと、を具備するようにした。

本発明のコンテンツ処理プログラムは、前記デジタル情報は、前記識別子に関連する情報を利用して暗号化されているようにした。

本発明のコンテンツ処理プログラムは、前記特定のデータは、なんらかの意味を持つ文字列、数値、画像、音声等のデータであるようにした。

本発明のコンテンツ処理プログラムは、前記識別子は、なんらかの意味を持つ文字列、数値、画像、音声等のデータであるようにした。

本発明のコンテンツ処理プログラムは、前記特定の環境または特定の識別子を持つ環境は、前記着脱可能なコンテンツ蓄積媒体を着脱することのできる特定の機器であるようにした。

本発明のコンテンツ処理プログラムは、前記特定の環境または特定の識別子を持つ環境は、特定のサービスと契約したことを示す識別子によって特定される環境であるようにした。

以上の構成によれば、コンテンツ蓄積媒体に格納された複数の暗号化コンテンツの判別を、当該暗号化コンテンツに関連付けられた情報に基づいて、一段と容易に行うようにすることができる。また、コンテンツ蓄積媒体に格納されているコンテンツが使用可能であるか否かを判断することが可能となり、正規

のデータでないデータを誤って再生してしまうといった不都合を防止することができる。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理プログラムであって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された暗号化データを読み出す暗号化データ読み出しステップと、前記読み出された暗号化データを自身の環境の識別子に関連する情報によって復号化し、特定のデータと合致するかどうかを判定する暗号化データ判別ステップと、を具備するようにした。

本発明のコンテンツ処理プログラムは、前記暗号化データ読み出しステップでは、前記暗号化された特定のデータは、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出されるようにした。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理プログラムであって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された識別子を読み出し、自身の環境の識別子と合致するかどうかを判定する識別子判別ステップ、を具備するようにした。

本発明のコンテンツ処理プログラムは、前記識別子判別ステップでは、前記識別子は、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ

蓄積媒体上の認証ファイルシステム内から読み出されるようにした。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理プログラムであって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された暗号化識別子を読み出す暗号化識別子読み出しステップと、前記読み出された暗号化識別子を自身の環境の特定の復号化手段によって復号化し、自身の識別子と合致するかどうかを判定する暗号化識別子判別ステップと、を具備するようにした。

本発明のコンテンツ処理プログラムは、前記暗号化識別子読み出しステップでは、前記暗号化識別子は、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出されるようにした。

本発明のコンテンツ処理プログラムは、さらに、前記暗号化識別子を特定の変換式に対応して変換する識別子逆変換ステップを具備し、前記暗号化識別子判別ステップでは、復号化された暗号化識別子は、前記識別子逆変換部で逆変換されてから自身の識別子と合致するか否かが判定されるようにした。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理プログラムであって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された固有データを読み出す固有データ読み出しステップと、前記読み出された固有データを自身の環境の固有データと合致するかどうかを判定する固有データ判別ステップと、を具備するよ

うにした。

本発明のコンテンツ処理プログラムは、前記固有データ読み出しステップでは、前記固有データは、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出されるようにした。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理プログラムであって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルと関連付けられた前記デジタル情報の書き込み時刻を読み出す書き込み時刻読み出しステップと、前記読み出された書き込み時刻と、自身の環境に格納されている書き込み時刻のひとつとが合致するか否かを判定する書き込み時刻判別ステップと、を具備するようにした。

本発明のコンテンツ処理プログラムは、前記書き込み時刻読み出しステップでは、前記書き込み時刻は、前記着脱可能なコンテンツ蓄積媒体と前記特定の環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出されるようにした。

本発明のコンテンツ処理プログラムは、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記書き込み時刻判別ステップでは、前記書き込み時刻読み出しステップで読み出された書き込み時刻が、自身の環境の持つ識別子に関連する情報を用いて復号されてから自身の環境に格納されている書き込み時刻のひとつと合致するか否か判定されるようにした。

本発明のコンテンツ処理プログラムは、さらに、前記書き込み時刻読み出しステップで読み出された書き込み時刻を、前記識別子に関連する情報を利用し

て変換する書き込み時刻変換ステップを具備し、前記書き込み時刻判別ステップでは、前記変換された書き込み時刻が特定の方法で復号されてから自身の環境に格納されている書き込み時刻のひとつと合致するか否かが判定されるようにした。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理プログラムであって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルと関連付けられた、ユーザによって指定されたユーザ指定値を読み出すユーザ指定値読み出しステップと、前記読み出されたユーザ指定値と、自身の環境に格納されているユーザ指定値が合致するか否かを判定するユーザ指定値判別ステップと、を具備するようにした。

本発明のコンテンツ処理プログラムは、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記ユーザ指定値判別ステップでは、前記ユーザ指定値読み出し部で読み出されたユーザ指定値は、自身の環境の持つ識別子に関連する情報を用いて復号されてから自身の環境に格納されているユーザ指定値と合致するか否かが判定されるようにした。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理プログラムであって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルと関連付けられた特定のデータを読み出す書き込み特定データ読み出しステップと、前記読み出された特定のデータと、自身の環境に格納されている特定のデータのひとつと合致するか否かを判定する書き込み特定デー

タ判別ステップと、を具備するようにした。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理プログラムであって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルの格納箇所である書き込み箇所を前記コンテンツ蓄積媒体上から読み出す書き込み箇所読み出しステップと、前記読み出された書き込み箇所と、自身の環境に格納されている書き込み箇所のひとつと合致するか否かを判定する書き込み箇所判別ステップと、を具備するようにした。

本発明のコンテンツ処理プログラムは、前記特定の環境または特定の識別子を持つ環境は、前記着脱可能なコンテンツ蓄積媒体を着脱することのできる特定の機器であるようにした。

本発明のコンテンツ処理プログラムは、前記特定の環境または特定の識別子を持つ環境は、特定のサービスと契約したことを示す識別子によって特定される環境であるようにした。

以上の構成によれば、コンテンツ蓄積媒体に格納された暗号化コンテンツを読み出し、復号化する前に、当該暗号化コンテンツに関連付けられた情報を基に、暗号化コンテンツを判別することにより、暗号化コンテンツを復号化することなく、その内容を容易に判別することができる。また、コンテンツ蓄積媒体に格納されているコンテンツが使用可能であるか否かを判断することが可能となり、正規のデータでないデータを誤って再生してしまうといった不都合を防止することができる。

本明細書は、２００２年３月２９日出願の特願２００２－０９７４２９に基づくものである。この内容をここに含めておく。

産業上の利用可能性

本発明は、例えばコンテンツ蓄積媒体を着脱可能な携帯端末装置に用いるに好適である。

請 求 の 範 囲

1．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報の前記コンテンツ蓄積媒体への書き込みを行うコンテンツ処理装置であって、

前記識別子又は前記識別子に関連する情報を暗号化の鍵として特定のデータを暗号化するデータ暗号化部と、

前記暗号化された特定のデータを前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化データ格納部と、

を具備するコンテンツ処理装置。

2．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記蓄積媒体に書き込むコンテンツ処理装置であって、

特定の暗号化手段を用いて前記識別子又は前記識別子に関連する情報を暗号化する識別子暗号化部と、

前記暗号化された識別子又は前記暗号化された関連する情報を前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化識別子格納部と、

を具備するコンテンツ処理装置。

3．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理装置であって、

前記特定の識別子とは異なる、前記特定の識別子を持つ環境に固有な特定のデータを、前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する固有データ格納部を具備するコンテンツ処理装置。

4．前記環境に固有な特定のデータは、ユーザが指定する値又は名称である請求の範囲３記載のコンテンツ処理装置。

5．前記コンテンツ処理装置は、さらに、ユーザが前記値又は名称を指定していない状態でその値又は名称として利用するための初期値をランダムに設定する初期値設定部を具備する請求の範囲４記載のコンテンツ処理装置。

6．前記コンテンツ処理装置は、さらに、前記値又は名称を前記識別子に関連する情報を用いて暗号化するユーザ指定値暗号化部を具備し、

前記固有データ格納部は、前記コンテンツ蓄積媒体に格納する値又は名称を、前記ユーザ指定値暗号化部によって暗号化されたものとする請求の範囲５記載のコンテンツ処理装置。

7．前記特定の識別子を持つ環境は、特定のサービスと契約したことを示す前記識別子によって特定される環境である請求の範囲１から６のいずれかに記載のコンテンツ処理装置。

8．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、

前記コンテンツ蓄積媒体上に前記デジタル情報のファイルと関連付けて格納された暗号化データを読み出す暗号化データ読み出し部と、

前記読み出された暗号化データを自身の環境の前記識別子又は自身の環境の前記識別子に関連する情報によって復号化し、特定のデータと合致するか否かを判定する暗号化データ判別部と、

を具備するコンテンツ処理装置。

9．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、

前記コンテンツ蓄積媒体上に前記デジタル情報のファイルと関連付けて格納された、前記識別子が暗号化されてなる暗号化識別子又は前記識別子に関連する情報が暗号化されてなる暗号化情報を読み出す暗号化識別子読み出し部と、

前記読み出された暗号化識別子又は暗号化情報を自身の環境の特定の復号化手段によって復号化し、自身の識別子又は識別子に関連する情報と合致するか否かを判定する暗号化識別子判別部と、

を具備するコンテンツ処理装置。

１０．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、

前記コンテンツ蓄積媒体上に前記デジタル情報のファイルと関連付けて格納された固有データを読み出す固有データ読み出し部と、

前記読み出された固有データが自身の環境に固有な特定のデータと合致するか否かを判定する固有データ判別部と、

を具備するコンテンツ処理装置。

１１．前記環境に固有な特定のデータは、ユーザによって指定されたユーザ指定値であり、前記固有データ判別部は、前記コンテンツ蓄積媒体から読み出された前記固有データと自身の環境に格納されている前記ユーザ指定値とが合致するか否かを判定する請求の範囲１０記載のコンテンツ処理装置。

１２．前記固有データ判別部は、前記読み出された固有データを、自身の環境の持つ前記識別子に関連する情報を用いて復号した後、当該復号された固有データが自身の環境に格納されている前記ユーザ指定値と合致するか否かを判定する請求の範囲１１記載のコンテンツ処理装置。

１３．前記特定の識別子を持つ環境は、特定のサービスと契約したことを示す前記識別子によって特定される環境である請求の範囲８から１２のいずれか

に記載のコンテンツ処理装置。

１４．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体であって、

前記識別子又は前記識別子に関連する情報を暗号化の鍵として暗号化された特定のデータが、前記デジタル情報のファイルと関連付けられて格納されているコンテンツ蓄積媒体。

１５．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体であって、

前記識別子が特定の暗号化手段によって暗号化されてなる暗号化識別子又は前記識別子に関連する情報が特定の暗号化手段によって暗号化されてなる暗号化情報が、前記デジタル情報のファイルと関連付けて格納されているコンテンツ蓄積媒体。

１６．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体であって、

前記特定の識別子とは異なる、前記特定の識別子を持つ環境に固有な特定のデータが、前記デジタル情報のファイルと関連付けられて格納されているコンテンツ蓄積媒体。

１７．前記環境に固有な特定のデータは、ユーザが指定した値又は名称である請求の範囲１６記載のコンテンツ蓄積媒体。

１８．前記ユーザが指定した値又は名称としては、ユーザがその値又は名称を指定していない状態では、初期値としてランダムな値が格納されている請求の

範囲１７記載のコンテンツ蓄積媒体。

１９．前記値又は名称は前記識別子に関連する情報を用いて暗号化されて格納されている請求の範囲１７記載のコンテンツ蓄積媒体。

２０．前記識別子は、特定のサービスと契約したことを示すデータである請求の範囲１４から１９のいずれかに記載のコンテンツ蓄積媒体。

２１．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報の前記コンテンツ蓄積媒体への書き込みを行うコンテンツ処理方法であって、

前記識別子又は前記識別子に関連する情報を暗号化の鍵として特定のデータを暗号化するデータ暗号化ステップと、

前記暗号化された特定のデータを前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化データ格納ステップと、

を具備するコンテンツ処理方法。

２２．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記蓄積媒体に書き込むコンテンツ処理方法であって、

特定の暗号化手段を用いて前記識別子又は前記識別子に関連する情報を暗号化する識別子暗号化ステップと、

前記暗号化された識別子又は前記暗号化された関連する情報を前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化識別子格納ステップと、

を備えるコンテンツ処理方法。

２３．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ

蓄積媒体に書き込むコンテンツ処理方法であって、

前記特定の識別子とは異なる、前記特定の識別子を持つ環境に固有な特定のデータを、前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する固有データ格納ステップを備えるコンテンツ処理方法。

２４．前記環境に固有な特定のデータは、ユーザが指定する値又は名称である請求の範囲２３記載のコンテンツ処理方法。

２５．前記コンテンツ処理方法は、さらに、ユーザが前記値又は名称を指定していない状態でその値又は名称として利用するための初期値をランダムに設定する初期値設定ステップを具備する請求の範囲２４記載のコンテンツ処理方法。

２６．前記コンテンツ処理方法は、さらに、前記値又は名称を前記識別子に関連する情報を用いて暗号化するユーザ指定値暗号化ステップを具備し、

前記固有データ格納ステップでは、前記コンテンツ蓄積媒体に格納する値又は名称が、前記ユーザ指定値暗号化ステップにおいて暗号化されたものとなる請求の範囲２４記載のコンテンツ処理方法。

２７．前記特定の識別子を持つ環境は、特定のサービスと契約したことを示す識別子によって特定される環境である請求の範囲２１から２６のいずれかに記載のコンテンツ処理方法。

２８．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、

前記コンテンツ蓄積媒体上に前記デジタル情報のファイルと関連付けて格納された暗号化データを読み出す暗号化データ読み出しステップと、

前記読み出された暗号化データを自身の環境の前記識別子又は自身の環境の前記識別子に関連する情報によって復号化し、特定のデータと合致するか否かを判定する暗号化データ判別ステップと、

を具備するコンテンツ処理方法。

２９．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、

前記コンテンツ蓄積媒体上に前記デジタル情報のファイルと関連付けて格納された、前記識別子が暗号化されてなる暗号化識別子又は前記識別子に関連する情報が暗号化されてなる暗号化情報を読み出す暗号化識別子読み出しステップと、

前記読み出された暗号化識別子又は暗号化情報を自身の環境の特定の復号化手段によって復号化し、自身の識別子又は識別子に関連する情報と合致するか否かを判定する暗号化識別子判別ステップと、

を具備するコンテンツ処理方法。

３０．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、

前記コンテンツ蓄積媒体上に前記デジタル情報のファイルと関連付けて格納された固有データを読み出す固有データ読み出しステップと、

前記読み出された固有データが自身の環境に固有な特定のデータと合致するか否かを判定する固有データ判別ステップと、

を具備するコンテンツ処理方法。

３１．前記環境に固有な特定のデータは、ユーザによって指定されたユーザ指定値であり、前記固有データ判別ステップでは、前記コンテンツ蓄積媒体から読み出された前記固有データと自身の環境に格納されている前記ユーザ指定値とが合致するか否かが判定される請求の範囲３０記載のコンテンツ処理方法。

３２．前記固有データ判別ステップでは、前記読み出した固有データを、読み出し先の環境が持つ前記識別子に関連する情報を用いて復号した後、当該復号された固有データが読み出し先の環境に格納されている前記ユーザ指定値と合致するか否か判定する請求の範囲３１記載のコンテンツ処理方法。

３３．前記特定の識別子を持つ環境は、特定のサービスと契約したことを示す前記識別子によって特定される環境である請求の範囲２８から３２のいずれかに記載のコンテンツ処理方法。

３４．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報の前記コンテンツ蓄積媒体への書き込みを行うためのコンテンツ処理プログラムであって、

前記識別子又は前記識別子に関連する情報を暗号化の鍵として特定のデータを暗号化するデータ暗号化ステップと、

前記暗号化された特定のデータを前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化データ格納ステップと、

を具備するコンテンツ処理プログラム。

３５．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記蓄積媒体に書き込むためのコンテンツ処理プログラムであって、

特定の暗号化手段を用いて前記識別子又は前記識別子に関連する情報を暗号化する識別子暗号化ステップと、

前記暗号化された識別子又は前記暗号化された関連する情報を前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化識別子格納ステップと、

を具備するコンテンツ処理プログラム。

３６．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むためのコンテンツ処理プログラムであって、

前記特定の識別子とは異なる、前記特定の識別子を持つ環境に固有な特定のデータを、前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する固有データ格納ステップを具備するコンテンツ処理プログラム。

３７．前記環境に固有な特定のデータは、ユーザが指定する値又は名称である請求の範囲３６記載のコンテンツ処理プログラム。

３８．前記コンテンツ処理プログラムは、さらに、ユーザが前記値又は名称を指定していない状態でその値又は名称として利用するための初期値をランダムに設定する初期値設定ステップを具備する請求の範囲３７記載のコンテンツ処理プログラム。

３９．前記コンテンツ処理プログラムは、さらに、前記値又は名称を前記識別子に関連する情報を用いて暗号化するユーザ指定値暗号化ステップを具備し、

前記固有データ格納ステップでは、前記コンテンツ蓄積媒体に格納する値又は名称が、前記ユーザ指定値暗号化ステップにおいて暗号化されたものとなる請求の範囲３７記載のコンテンツ処理プログラム。

４０．前記特定の識別子を持つ環境は、特定のサービスと契約したことを示す識別子によって特定される環境である請求の範囲３４から３９のいずれかに記載のコンテンツ処理プログラム。

４１．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すためのコンテンツ処理プログラムであって、

前記コンテンツ蓄積媒体上に前記デジタル情報のファイルと関連付けて格納された暗号化データを読み出す暗号化データ読み出しステップと、

前記読み出された暗号化データを自身の環境の前記識別子又は自身の環境の前記識別子に関連する情報によって復号化し、特定のデータと合致するか否かを判定する暗号化データ判別ステップと、

を具備するコンテンツ処理プログラム。

４２．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すためのコンテンツ処理プログラムであって、

前記コンテンツ蓄積媒体上に前記デジタル情報のファイルと関連付けて格納された、前記識別子が暗号化されてなる暗号化識別子又は前記識別子に関連する情報が暗号化されてなる暗号化情報を読み出す暗号化識別子読み出しステップと、

前記読み出された暗号化識別子又は暗号化情報を自身の環境の特定の復号化手段によって復号化し、自身の識別子又は識別子に関連する情報と合致するか否かを判定する暗号化識別子判別ステップと、

を具備するコンテンツ処理プログラム。

４３．デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すためのコンテンツ処理プログラムであって、

前記コンテンツ蓄積媒体上に前記デジタル情報のファイルと関連付けて格納された固有データを読み出す固有データ読み出しステップと、

前記読み出された固有データが自身の環境に固有な特定のデータと合致するか否かを判定する固有データ判別ステップと、

を具備するコンテンツ処理プログラム。

４４．前記環境に固有な特定のデータは、ユーザによって指定されたユーザ指定値であり、前記固有データ判別ステップでは、前記コンテンツ蓄積媒体から

読み出された前記固有データと自身の環境に格納されている前記ユーザ指定値とが合致するか否かが判定される請求の範囲４３記載のコンテンツ処理プログラム。

４５．前記固有データ判別ステップは、前記読み出した固有データを、読み出し先の環境が持つ前記識別子に関連する情報を用いて復号した後、当該復号された固有データが読み出し先の環境に格納されている前記ユーザ指定値と合致するか否か判定する請求の範囲４４記載のコンテンツ処理プログラム。

４６．前記特定の識別子を持つ環境は、特定のサービスと契約したことを示す前記識別子によって特定される環境である請求の範囲４１から４５のいずれかに記載のコンテンツ処理プログラム。

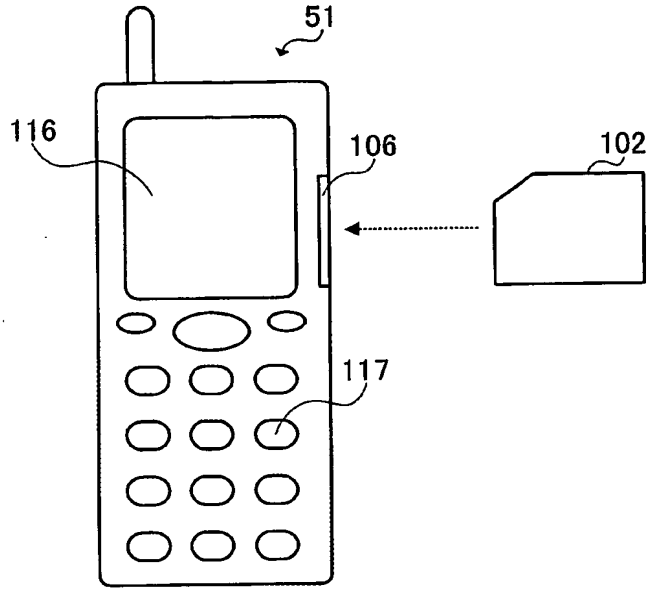


図 1

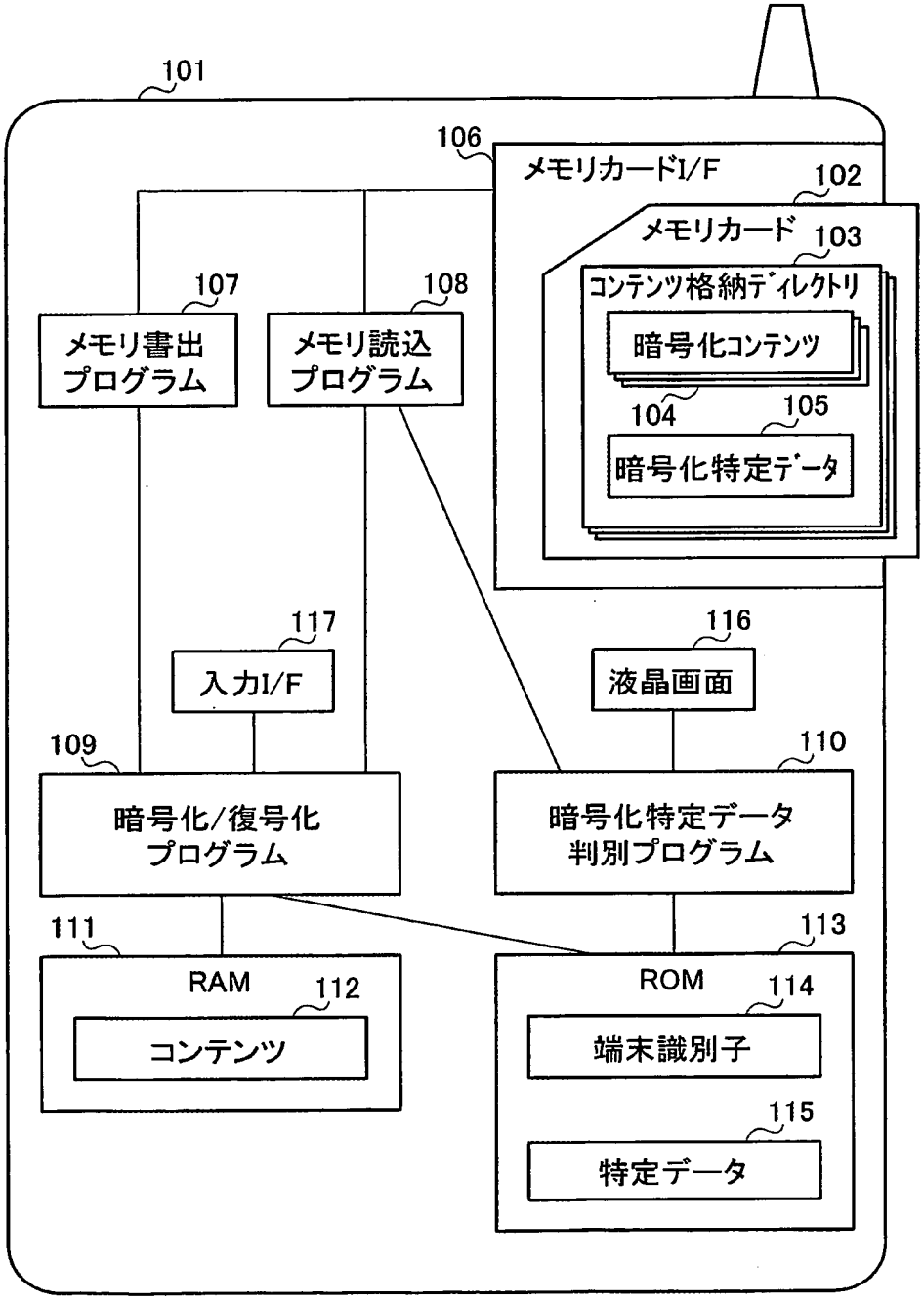

101
106
メモリカードI/F
102
メモリカード
103
コンテンツ格納ディレクトリ
暗号化コンテンツ
104
105
暗号化特定データ
107
メモリ書出
プログラム
108
メモリ読込
プログラム
117
入力I/F
116
液晶画面
109
暗号化/復号化
プログラム
110
暗号化特定データ
判別プログラム
111
RAM
112
コンテンツ
113
ROM
114
端末識別子
115
特定データ

図 2

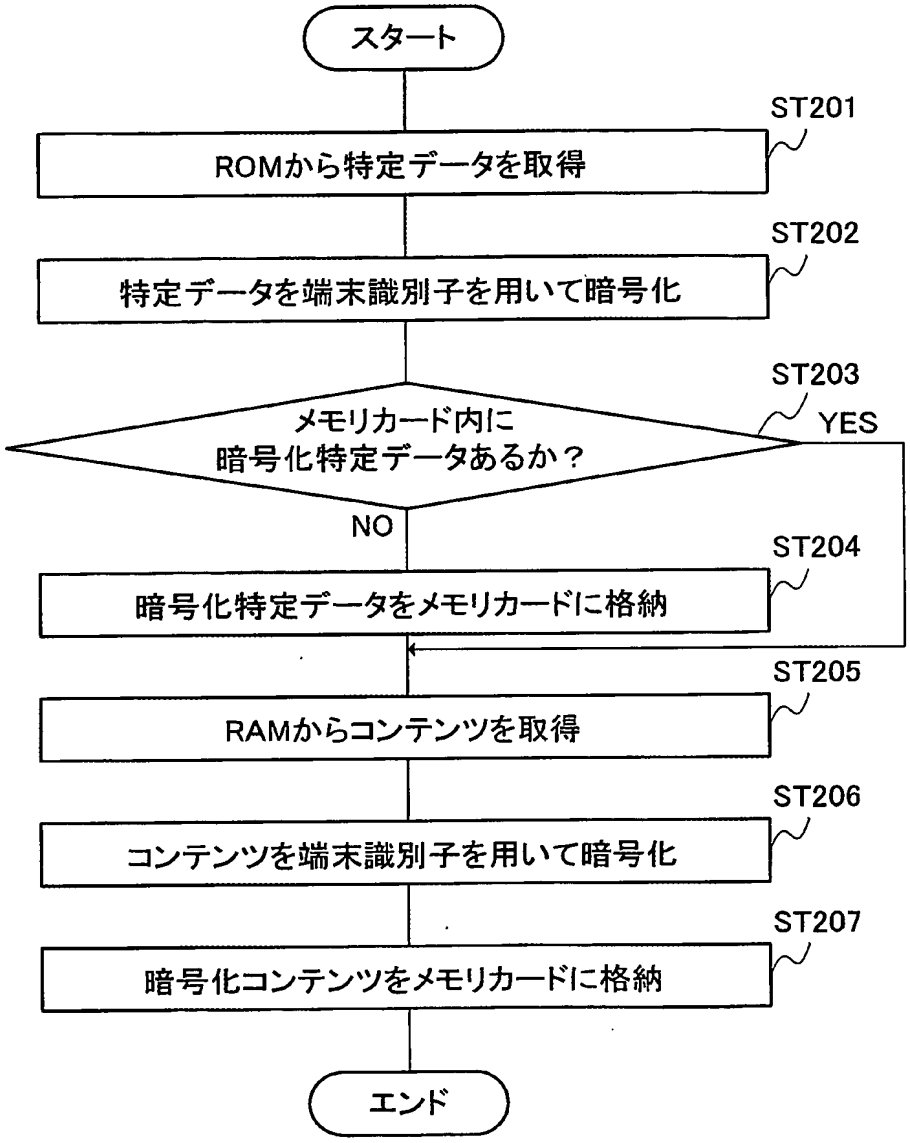

スタート
ST201
ROMから特定データを取得
ST202
特定データを端末識別子を用いて暗号化
ST203
メモリカード内に
暗号化特定データあるか？
YES
NO
ST204
暗号化特定データをメモリカードに格納
ST205
RAMからコンテンツを取得
ST206
コンテンツを端末識別子を用いて暗号化
ST207
暗号化コンテンツをメモリカードに格納
エンド

図 3

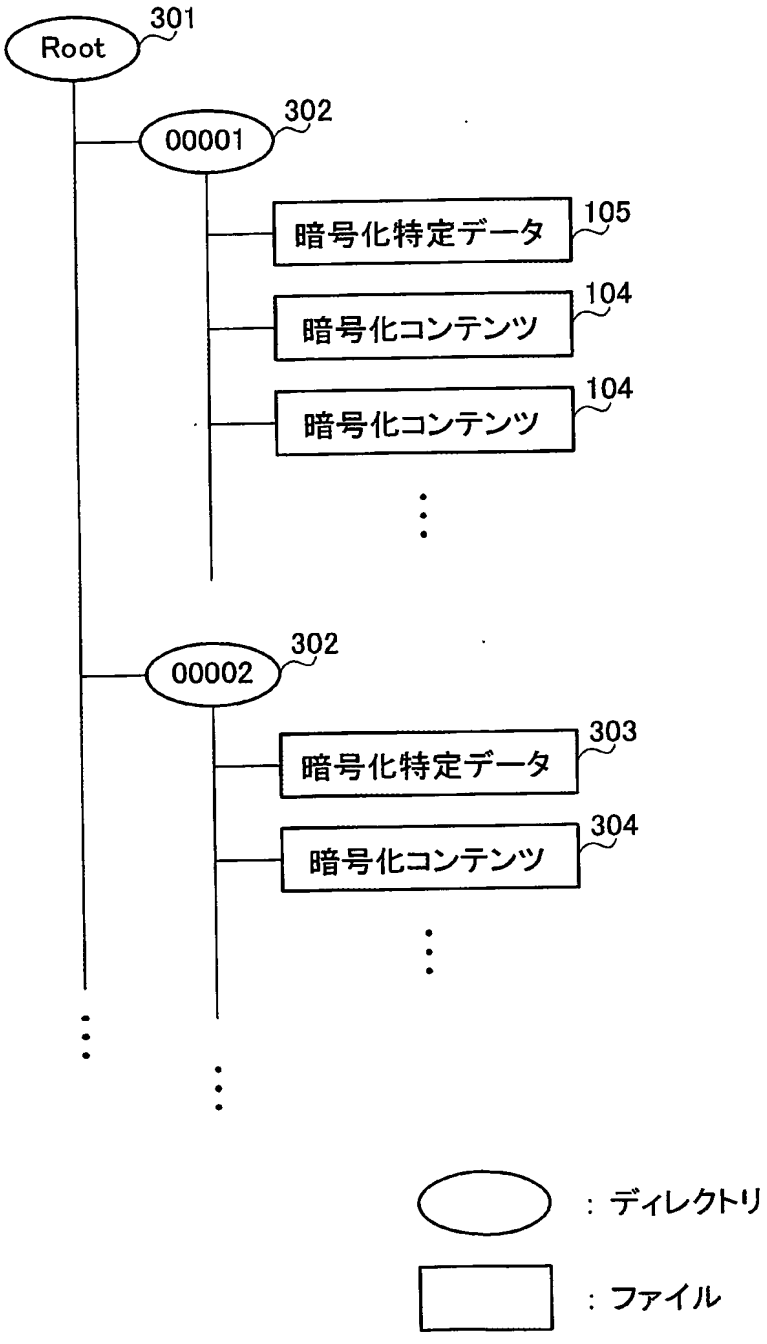

Root
301
00001
302
暗号化特定データ
105
暗号化コンテンツ
104
暗号化コンテンツ
104
00002
302
暗号化特定データ
303
暗号化コンテンツ
304
：ディレクトリ
：ファイル

図 4

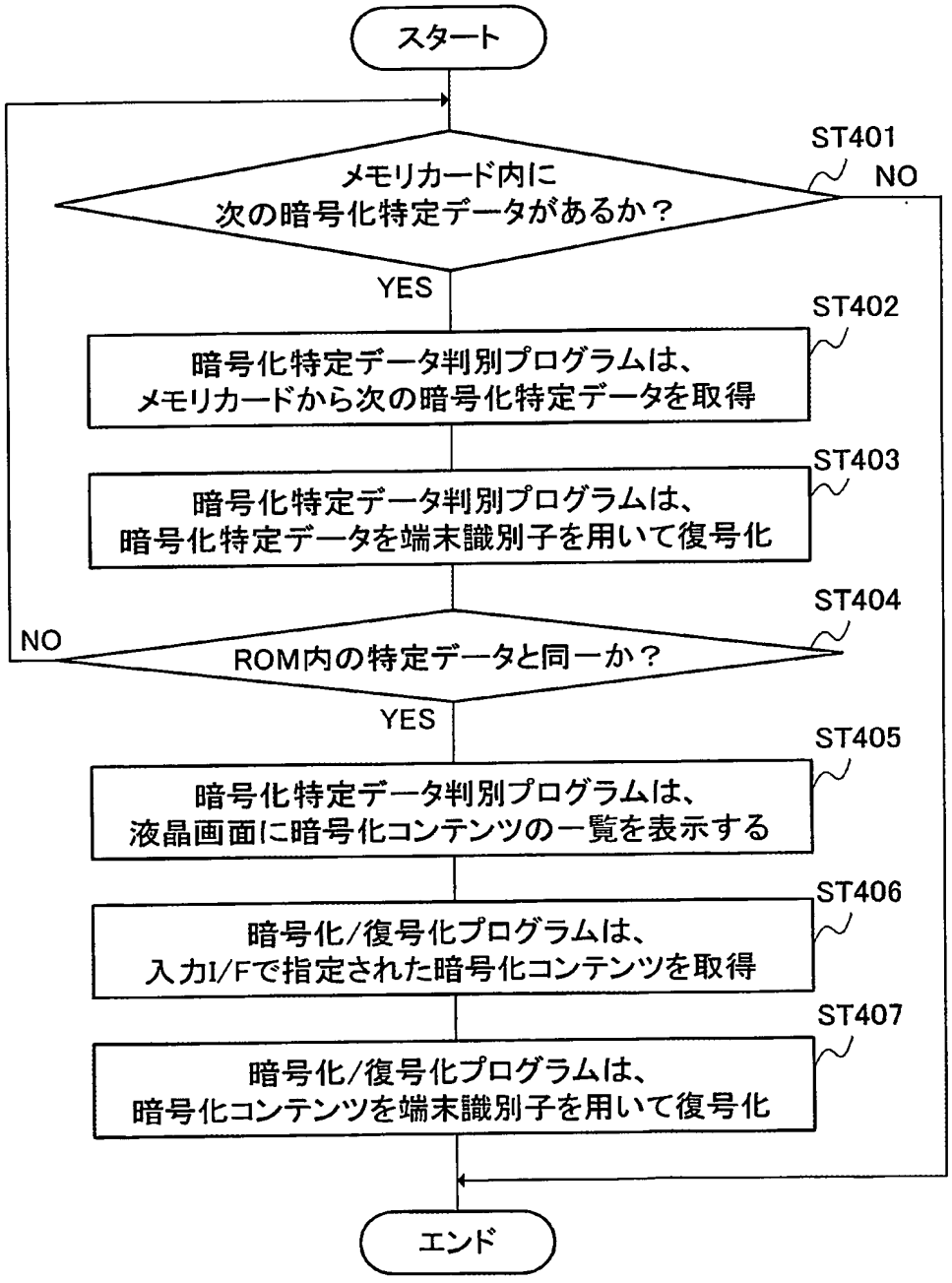

スタート
ST401
メモリカード内に
次の暗号化特定データがあるか？
NO
YES
ST402
暗号化特定データ判別プログラムは、
メモリカードから次の暗号化特定データを取得
ST403
暗号化特定データ判別プログラムは、
暗号化特定データを端末識別子を用いて復号化
ST404
NO
ROM内の特定データと同一か？
YES
ST405
暗号化特定データ判別プログラムは、
液晶画面に暗号化コンテンツの一覧を表示する
ST406
暗号化/復号化プログラムは、
入力I/Fで指定された暗号化コンテンツを取得
ST407
暗号化/復号化プログラムは、
暗号化コンテンツを端末識別子を用いて復号化
エンド

図 5

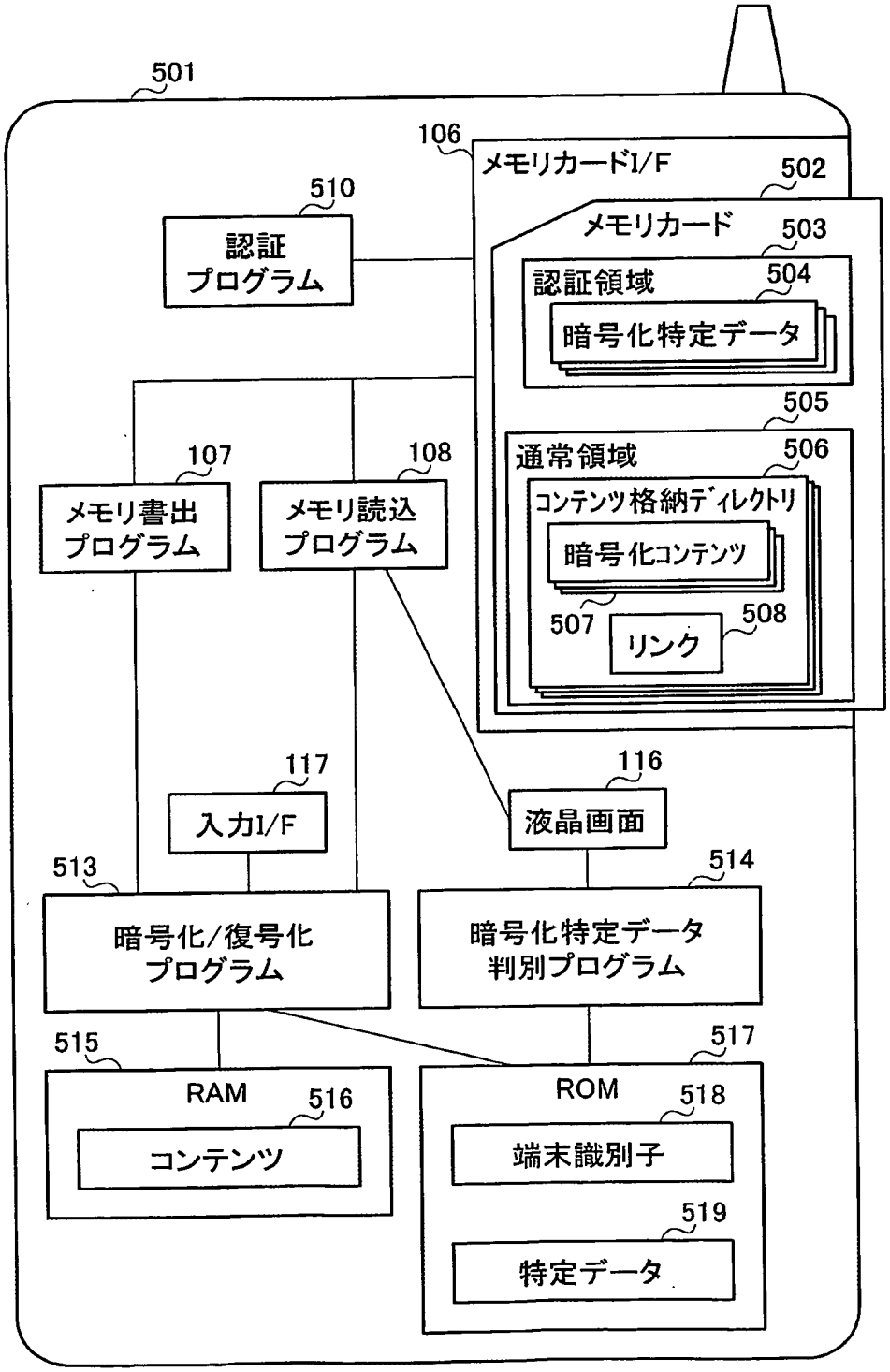

501
106
メモリカードI/F
502
510
認証
プログラム
メモリカード
503
認証領域
504
暗号化特定データ
505
通常領域
506
コンテンツ格納ディレクトリ
暗号化コンテンツ
507
508
リンク
107
メモリ書出
プログラム
108
メモリ読込
プログラム
117
入力I/F
116
液晶画面
513
暗号化/復号化
プログラム
514
暗号化特定データ
判別プログラム
515
RAM
516
コンテンツ
517
ROM
518
端末識別子
519
特定データ

図 6

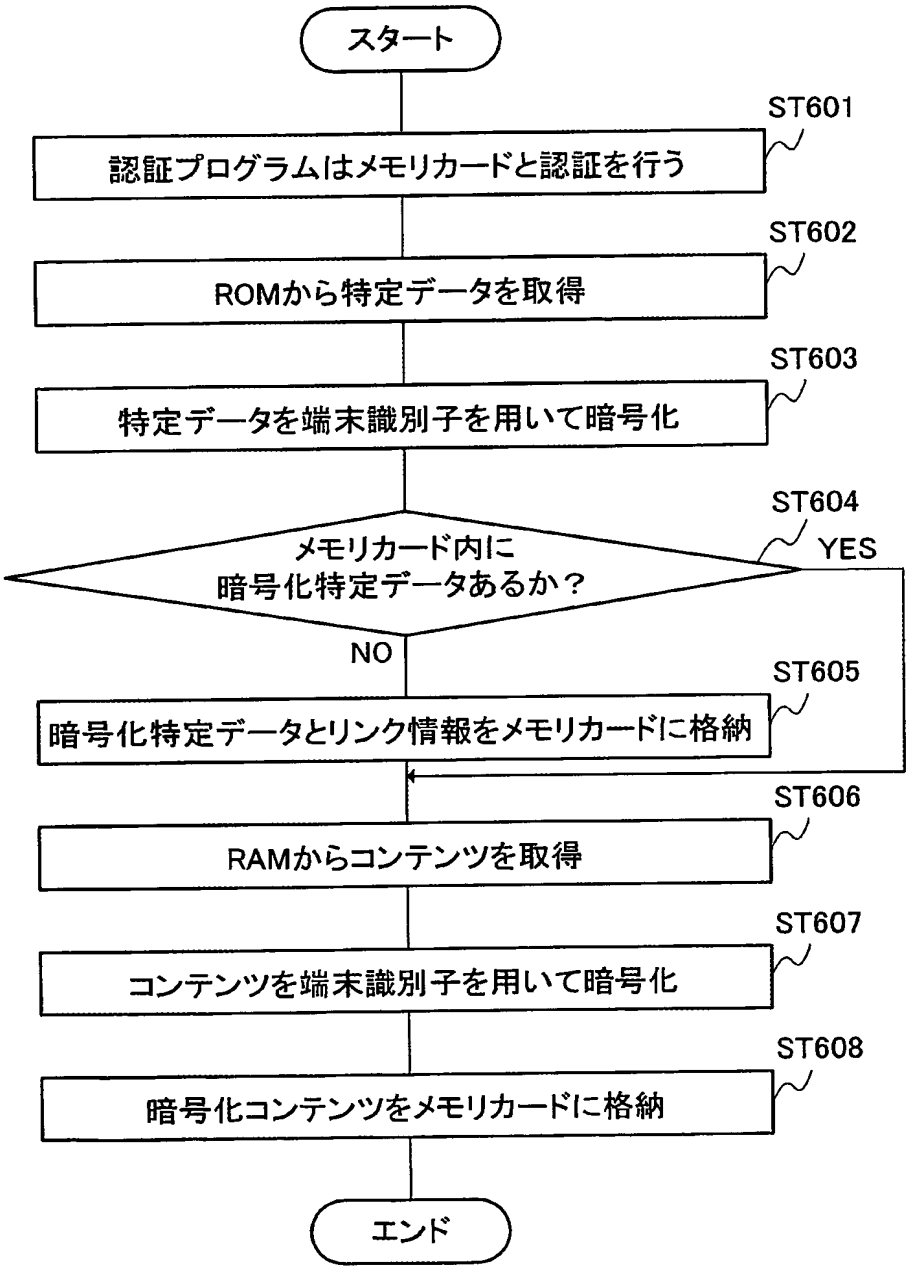

スタート
ST601
認証プログラムはメモリカードと認証を行う
ST602
ROMから特定データを取得
ST603
特定データを端末識別子を用いて暗号化
ST604
メモリカード内に
暗号化特定データあるか？
YES
NO
ST605
暗号化特定データとリンク情報をメモリカードに格納
ST606
RAMからコンテンツを取得
ST607
コンテンツを端末識別子を用いて暗号化
ST608
暗号化コンテンツをメモリカードに格納
エンド

図 7

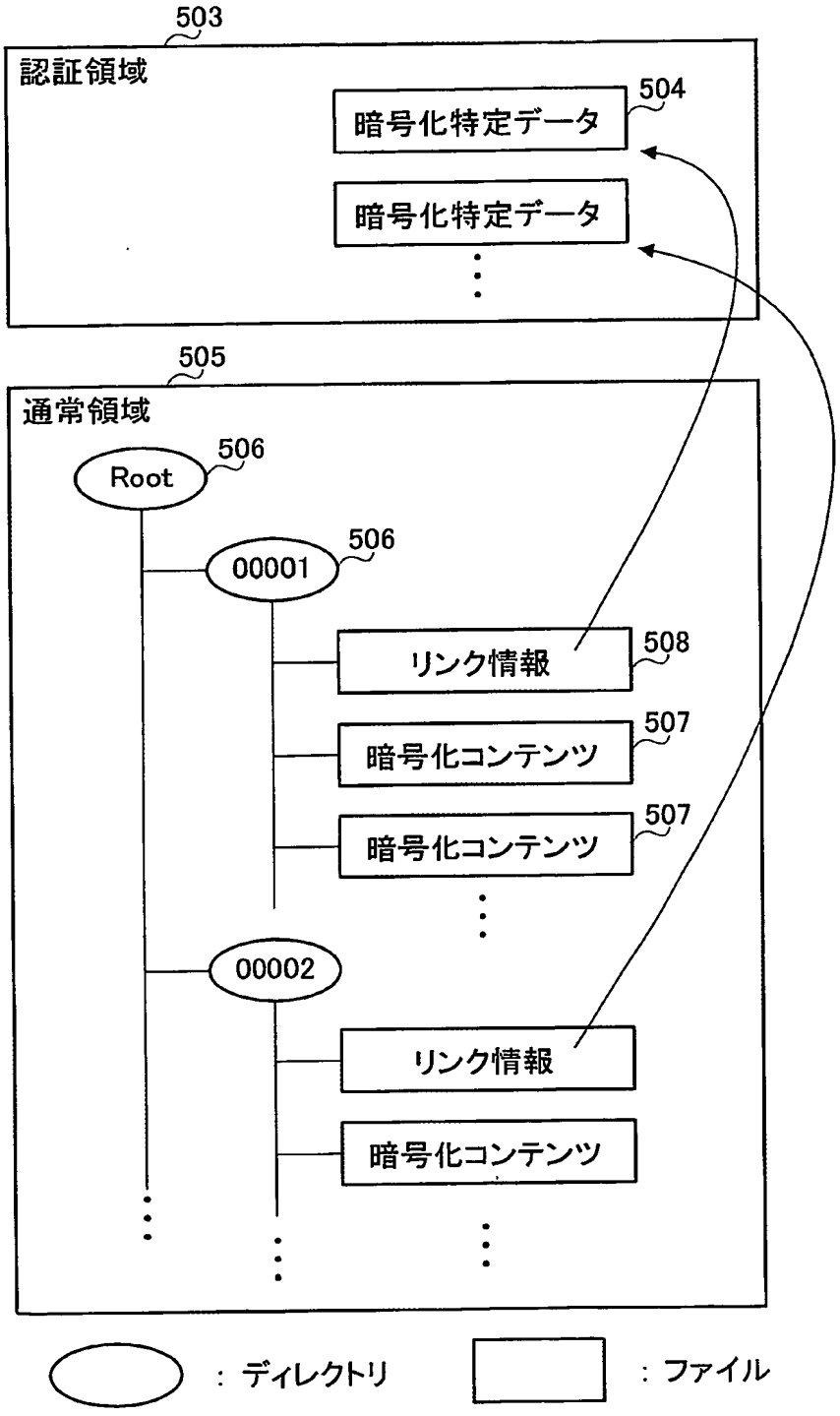

503
認証領域
504
暗号化特定データ
暗号化特定データ
505
通常領域
506
Root
506
00001
508
リンク情報
507
暗号化コンテンツ
507
暗号化コンテンツ
00002
リンク情報
暗号化コンテンツ
：ディレクトリ
：ファイル

図 8

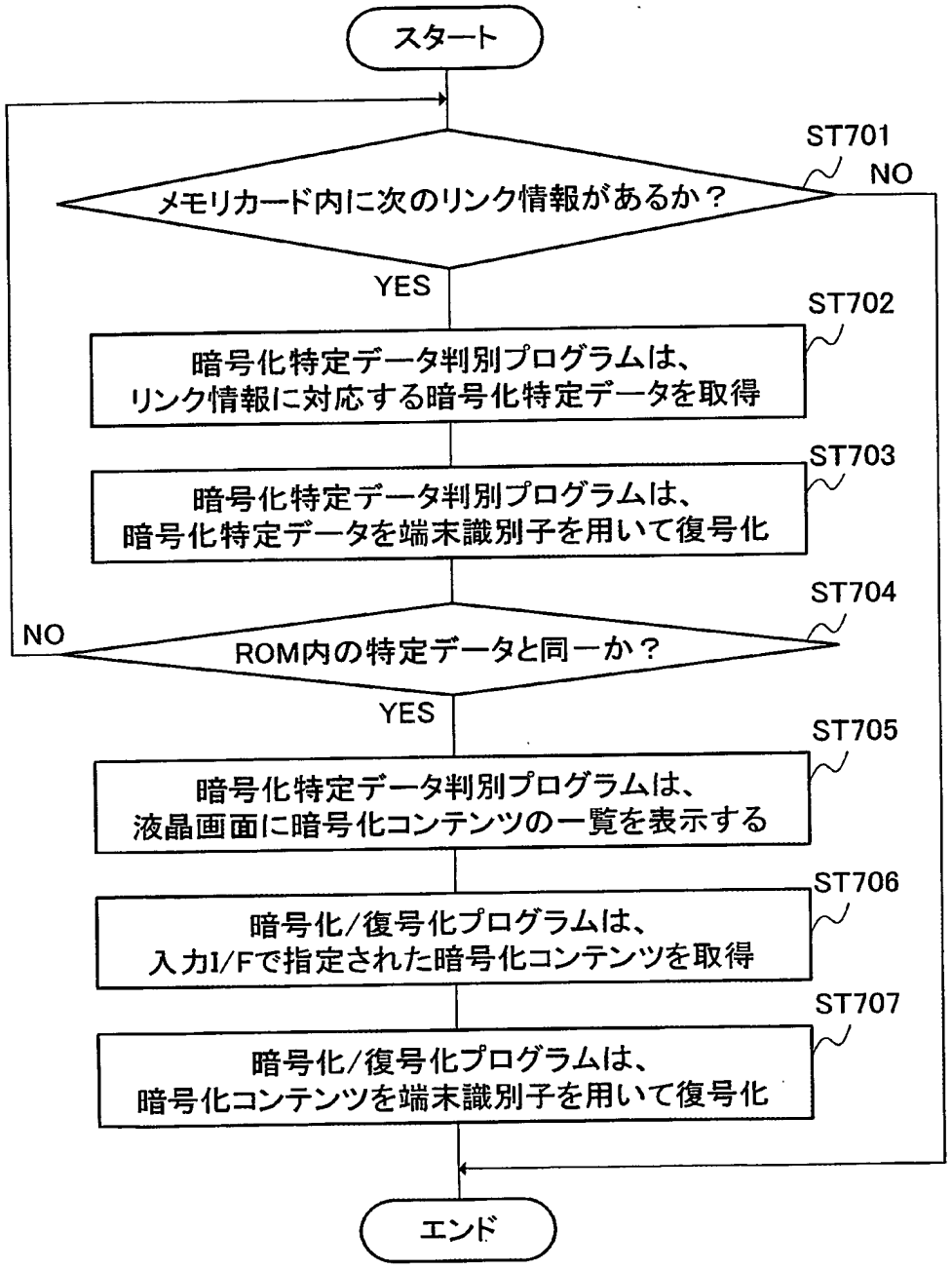

スタート
ST701
メモリカード内に次のリンク情報があるか？
NO
YES
ST702
暗号化特定データ判別プログラムは、
リンク情報に対応する暗号化特定データを取得
ST703
暗号化特定データ判別プログラムは、
暗号化特定データを端末識別子を用いて復号化
ST704
NO
ROM内の特定データと同一か？
YES
ST705
暗号化特定データ判別プログラムは、
液晶画面に暗号化コンテンツの一覧を表示する
ST706
暗号化/復号化プログラムは、
入力I/Fで指定された暗号化コンテンツを取得
ST707
暗号化/復号化プログラムは、
暗号化コンテンツを端末識別子を用いて復号化
エンド

図 9

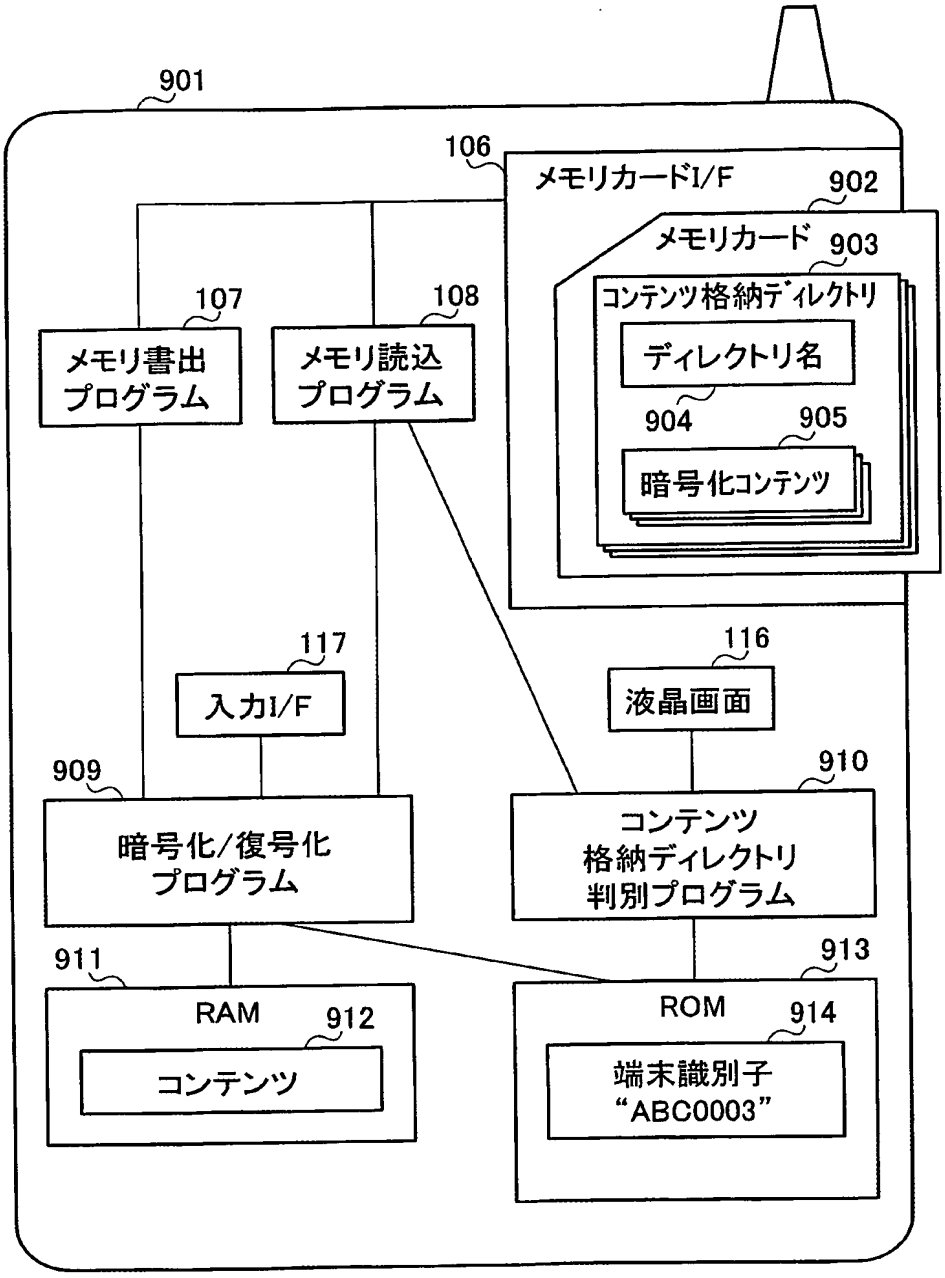

901
106
メモリカードI/F
902
メモリカード
903
コンテンツ格納ディレクトリ
ディレクトリ名
904
905
暗号化コンテンツ
107
メモリ書出
プログラム
108
メモリ読込
プログラム
117
入力I/F
116
液晶画面
909
暗号化/復号化
プログラム
910
コンテンツ
格納ディレクトリ
判別プログラム
911
RAM
912
コンテンツ
913
ROM
914
端末識別子
“ABC0003”

図 10

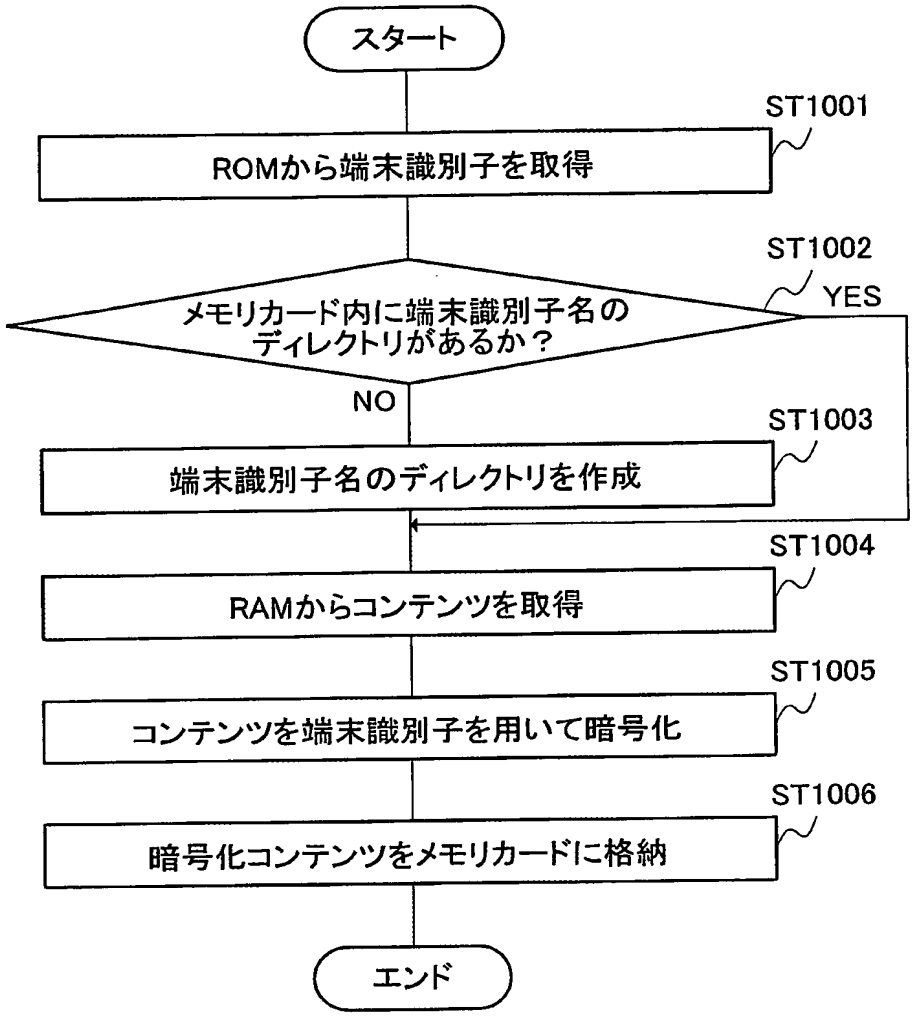

スタート
ST1001
ROMから端末識別子を取得
ST1002
メモリカード内に端末識別子名のディレクトリがあるか？
YES
NO
ST1003
端末識別子名のディレクトリを作成
ST1004
RAMからコンテンツを取得
ST1005
コンテンツを端末識別子を用いて暗号化
ST1006
暗号化コンテンツをメモリカードに格納
エンド

図 11

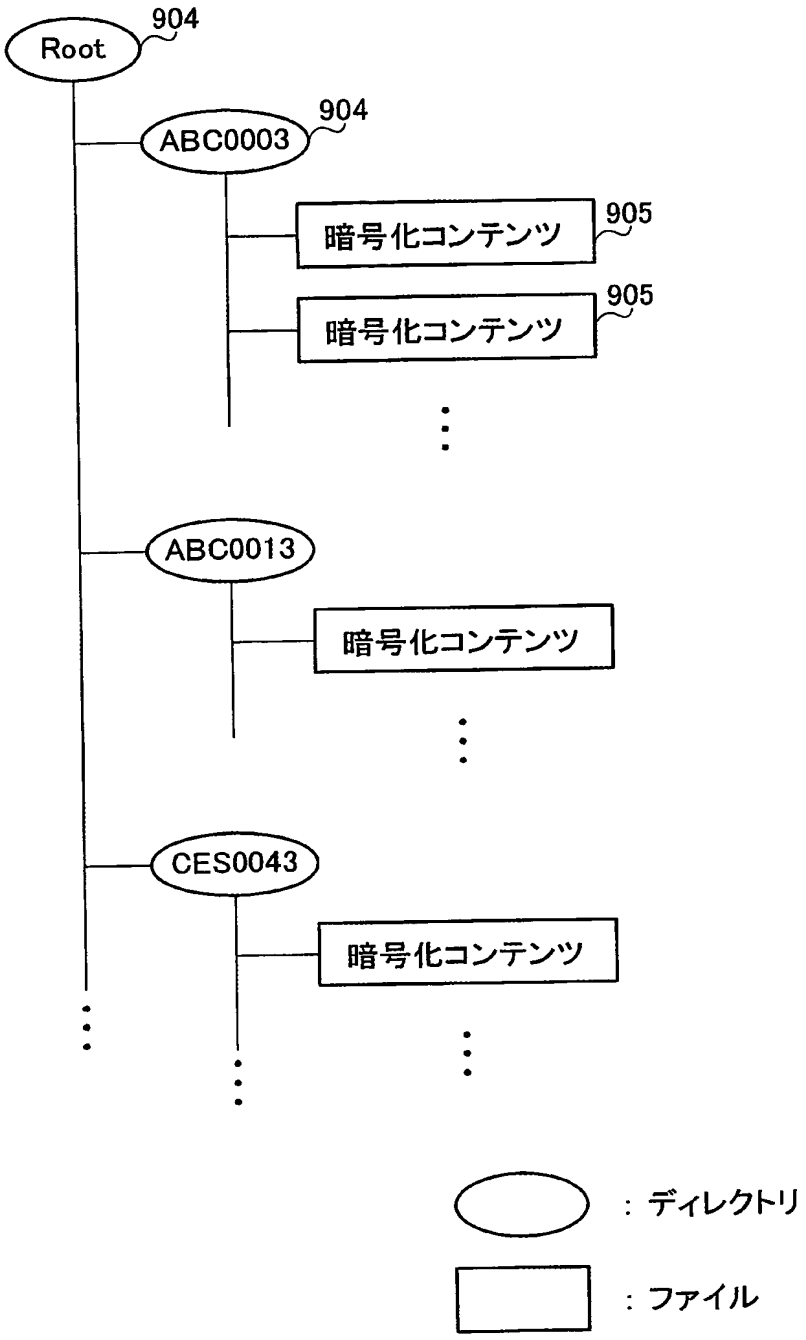

Root
904
ABC0003
904
暗号化コンテンツ
905
暗号化コンテンツ
905
ABC0013
暗号化コンテンツ
CES0043
暗号化コンテンツ
：ディレクトリ
：ファイル

図 12

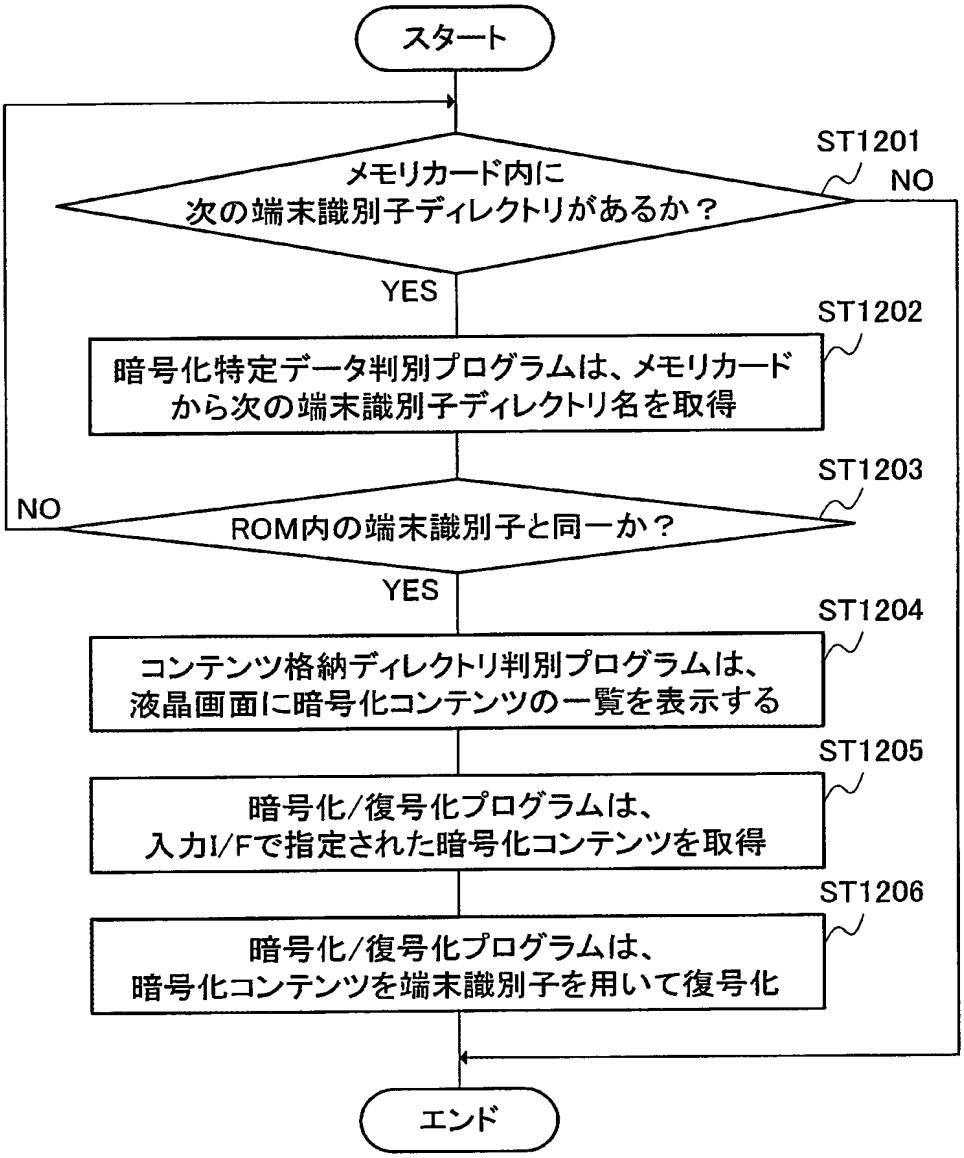

スタート
ST1201
メモリカード内に
次の端末識別子ディレクトリがあるか？
NO
YES
ST1202
暗号化特定データ判別プログラムは、メモリカード
から次の端末識別子ディレクトリ名を取得
ST1203
NO
ROM内の端末識別子と同一か？
YES
ST1204
コンテンツ格納ディレクトリ判別プログラムは、
液晶画面に暗号化コンテンツの一覧を表示する
ST1205
暗号化/復号化プログラムは、
入力I/Fで指定された暗号化コンテンツを取得
ST1206
暗号化/復号化プログラムは、
暗号化コンテンツを端末識別子を用いて復号化
エンド

図 13

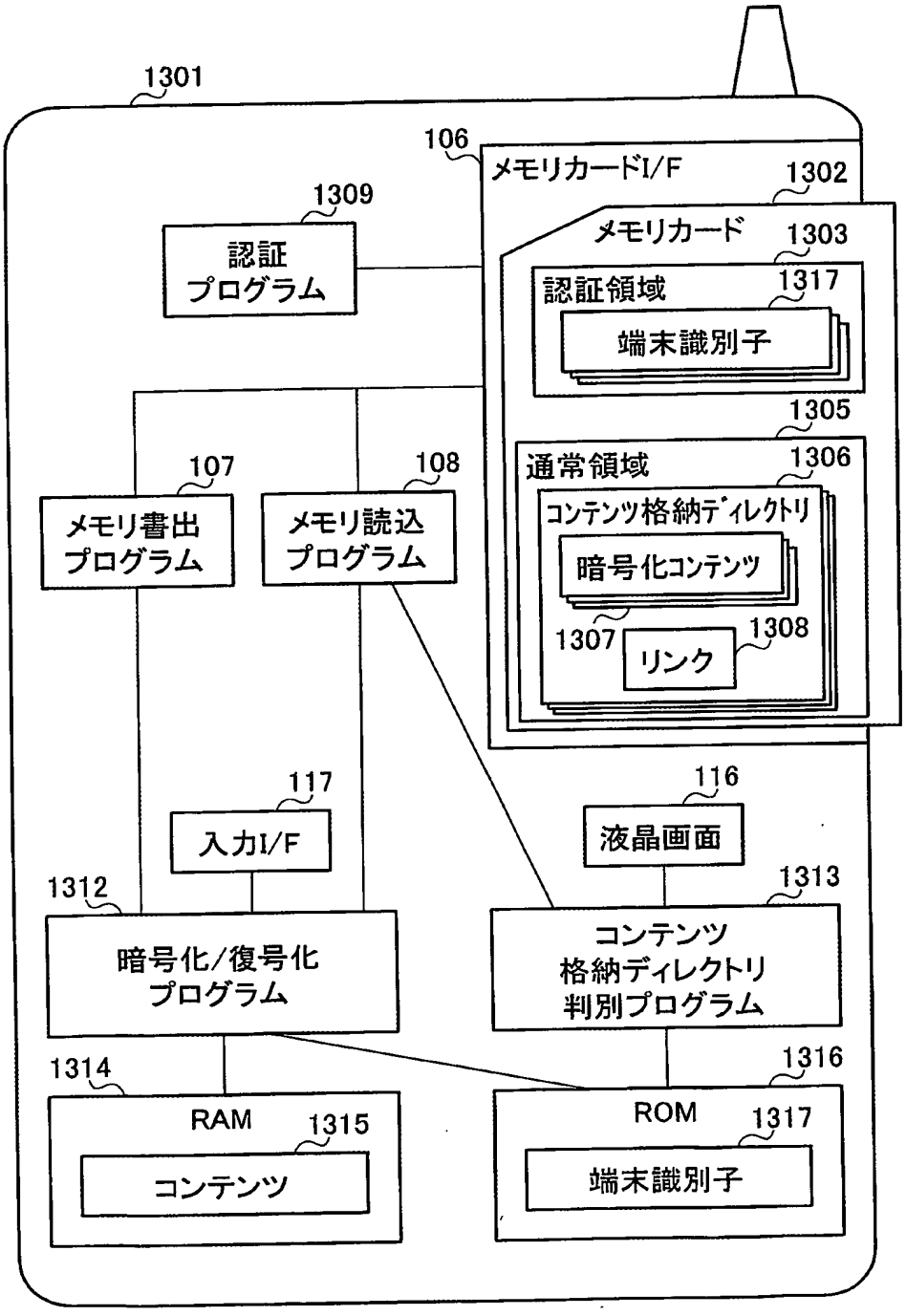

1301
106
メモリカードI/F
1302
1309
認証
プログラム
メモリカード
1303
認証領域
1317
端末識別子
1305
通常領域
1306
107
108
メモリ書出
プログラム
メモリ読込
プログラム
コンテンツ格納ディレクトリ
暗号化コンテンツ
1307
1308
リンク
117
116
入力I/F
液晶画面
1312
1313
暗号化/復号化
プログラム
コンテンツ
格納ディレクトリ
判別プログラム
1314
1316
RAM
1315
ROM
1317
コンテンツ
端末識別子

図 14

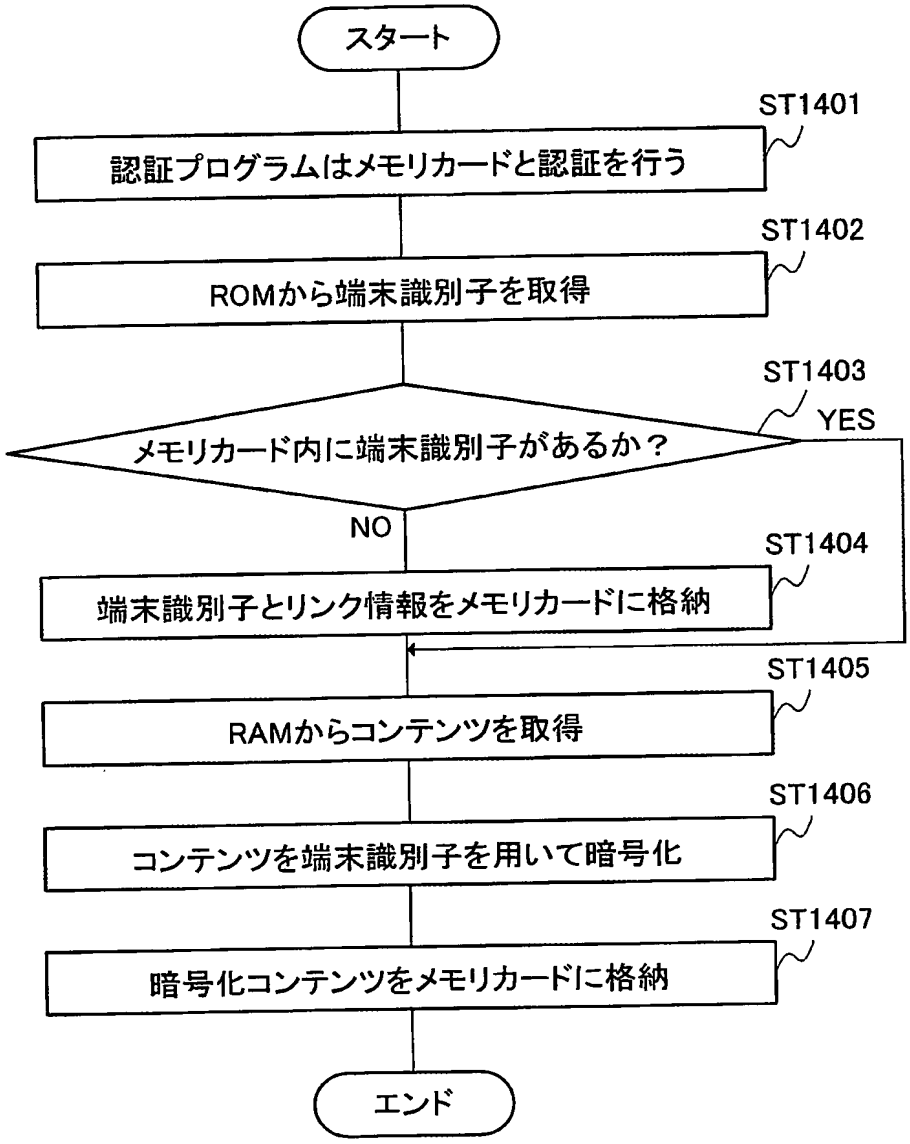

スタート
ST1401
認証プログラムはメモリカードと認証を行う
ST1402
ROMから端末識別子を取得
ST1403
メモリカード内に端末識別子があるか？
YES
NO
ST1404
端末識別子とリンク情報をメモリカードに格納
ST1405
RAMからコンテンツを取得
ST1406
コンテンツを端末識別子を用いて暗号化
ST1407
暗号化コンテンツをメモリカードに格納
エンド

図 15

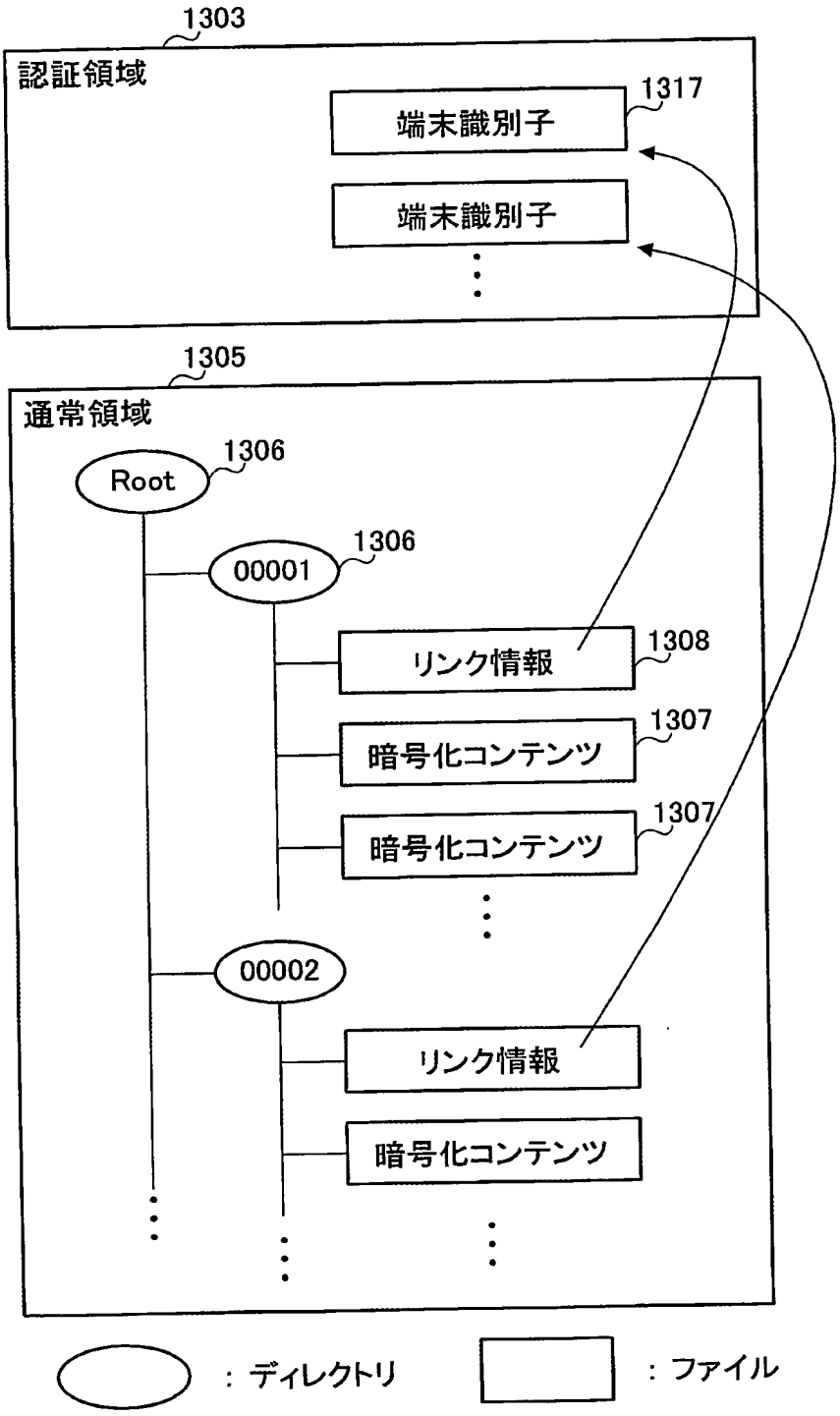

1303
認証領域
1317
端末識別子
端末識別子
1305
通常領域
1306
Root
1306
00001
リンク情報
1308
暗号化コンテンツ
1307
暗号化コンテンツ
1307
00002
リンク情報
暗号化コンテンツ
：ディレクトリ
：ファイル

図 16

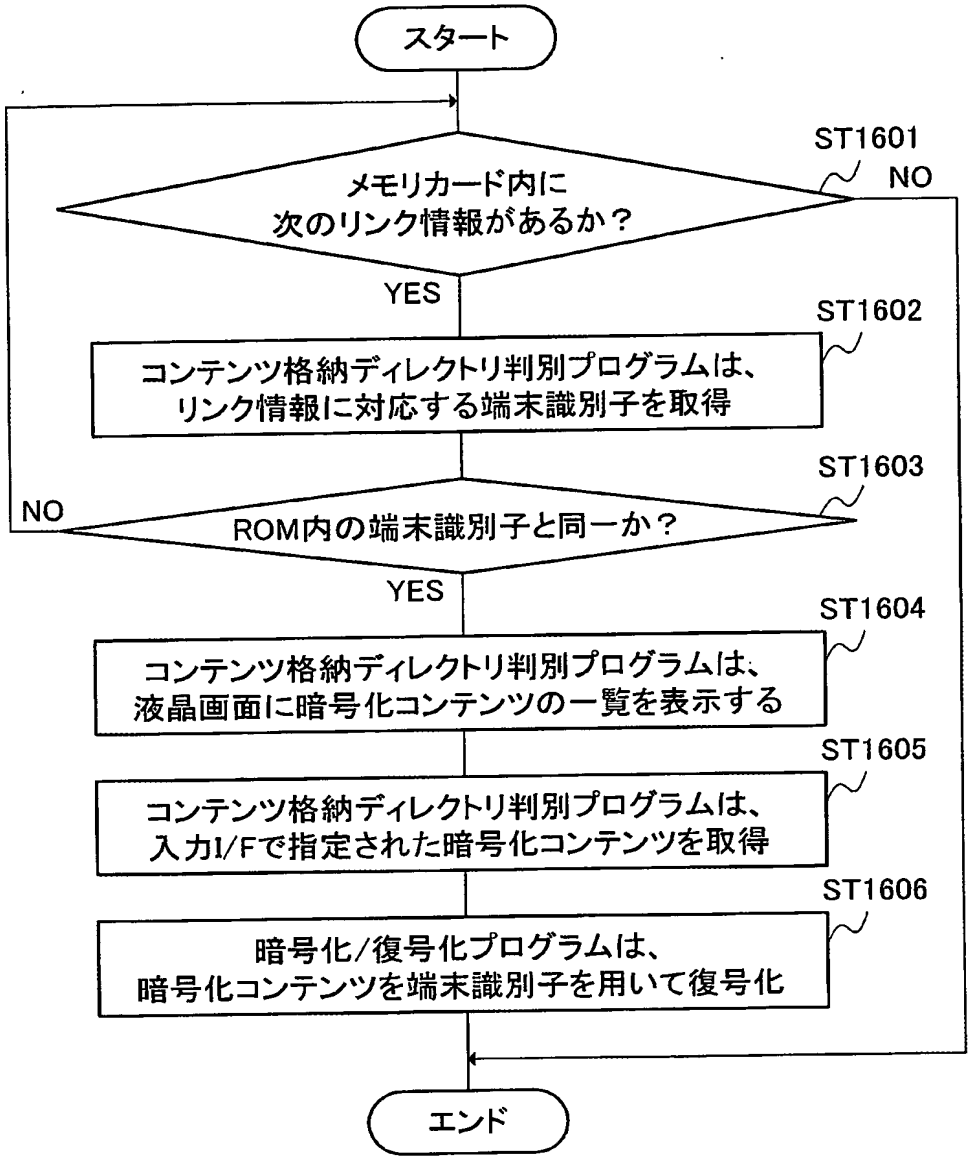

スタート
ST1601
メモリカード内に
次のリンク情報があるか？
NO
YES
ST1602
コンテンツ格納ディレクトリ判別プログラムは、
リンク情報に対応する端末識別子を取得
ST1603
NO
ROM内の端末識別子と同一か？
YES
ST1604
コンテンツ格納ディレクトリ判別プログラムは、
液晶画面に暗号化コンテンツの一覧を表示する
ST1605
コンテンツ格納ディレクトリ判別プログラムは、
入力I/Fで指定された暗号化コンテンツを取得
ST1606
暗号化/復号化プログラムは、
暗号化コンテンツを端末識別子を用いて復号化
エンド

図 17

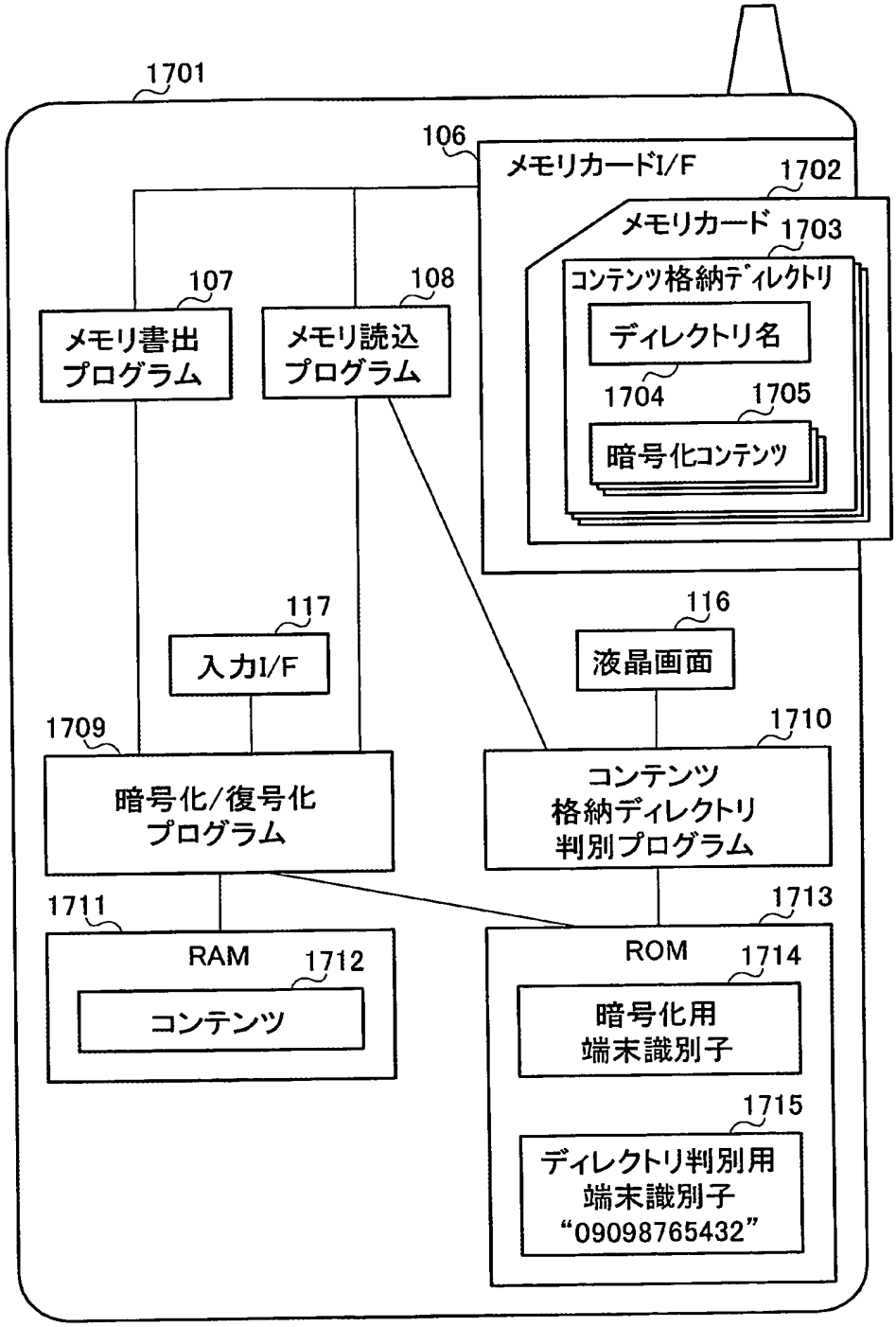

1701
106
メモリカードI/F
1702
メモリカード
1703
コンテンツ格納ディレクトリ
ディレクトリ名
1704
1705
暗号化コンテンツ
107
メモリ書出
プログラム
108
メモリ読込
プログラム
117
入力I/F
116
液晶画面
1709
暗号化/復号化
プログラム
1710
コンテンツ
格納ディレクトリ
判別プログラム
1711
RAM
1712
コンテンツ
1713
ROM
1714
暗号化用
端末識別子
1715
ディレクトリ判別用
端末識別子
“09098765432”

図 18

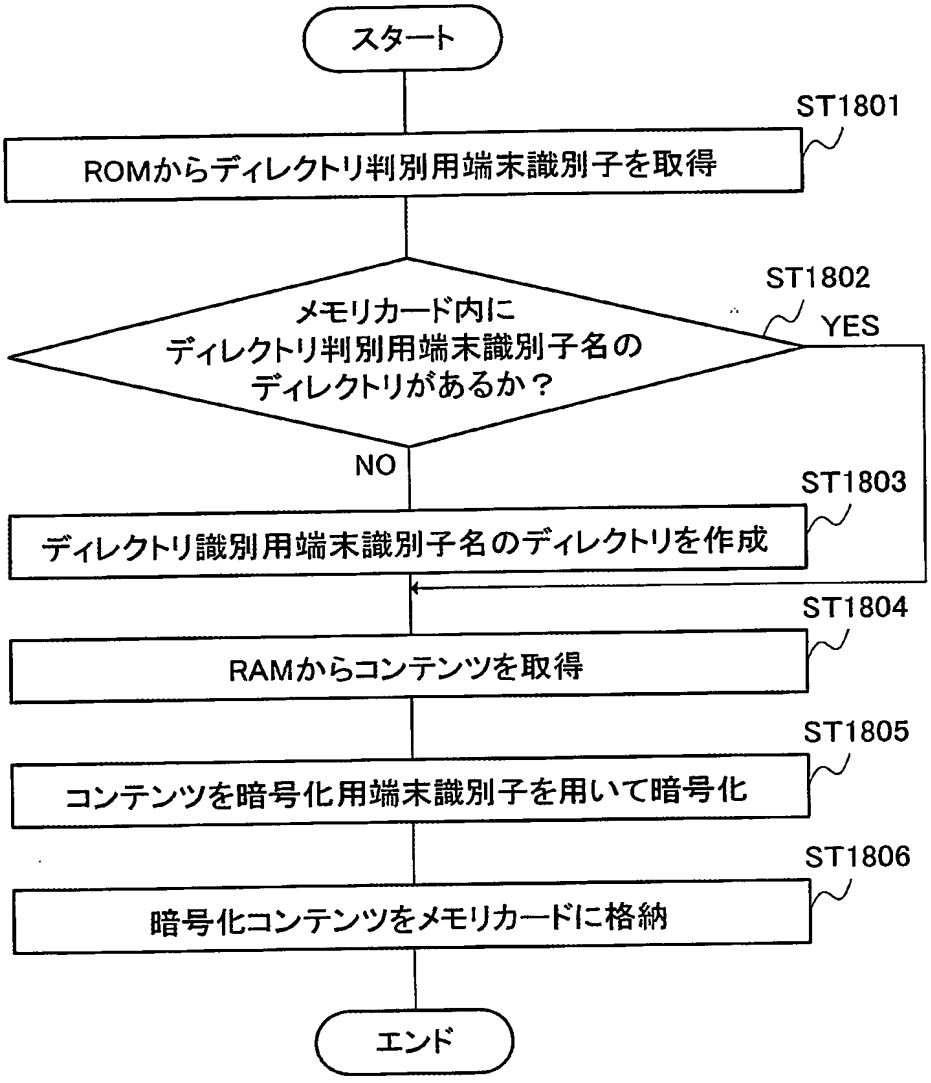

スタート
ST1801
ROMからディレクトリ判別用端末識別子を取得
ST1802
メモリカード内に
ディレクトリ判別用端末識別子名の
ディレクトリがあるか？
YES
NO
ST1803
ディレクトリ識別用端末識別子名のディレクトリを作成
ST1804
RAMからコンテンツを取得
ST1805
コンテンツを暗号化用端末識別子を用いて暗号化
ST1806
暗号化コンテンツをメモリカードに格納
エンド

図 19

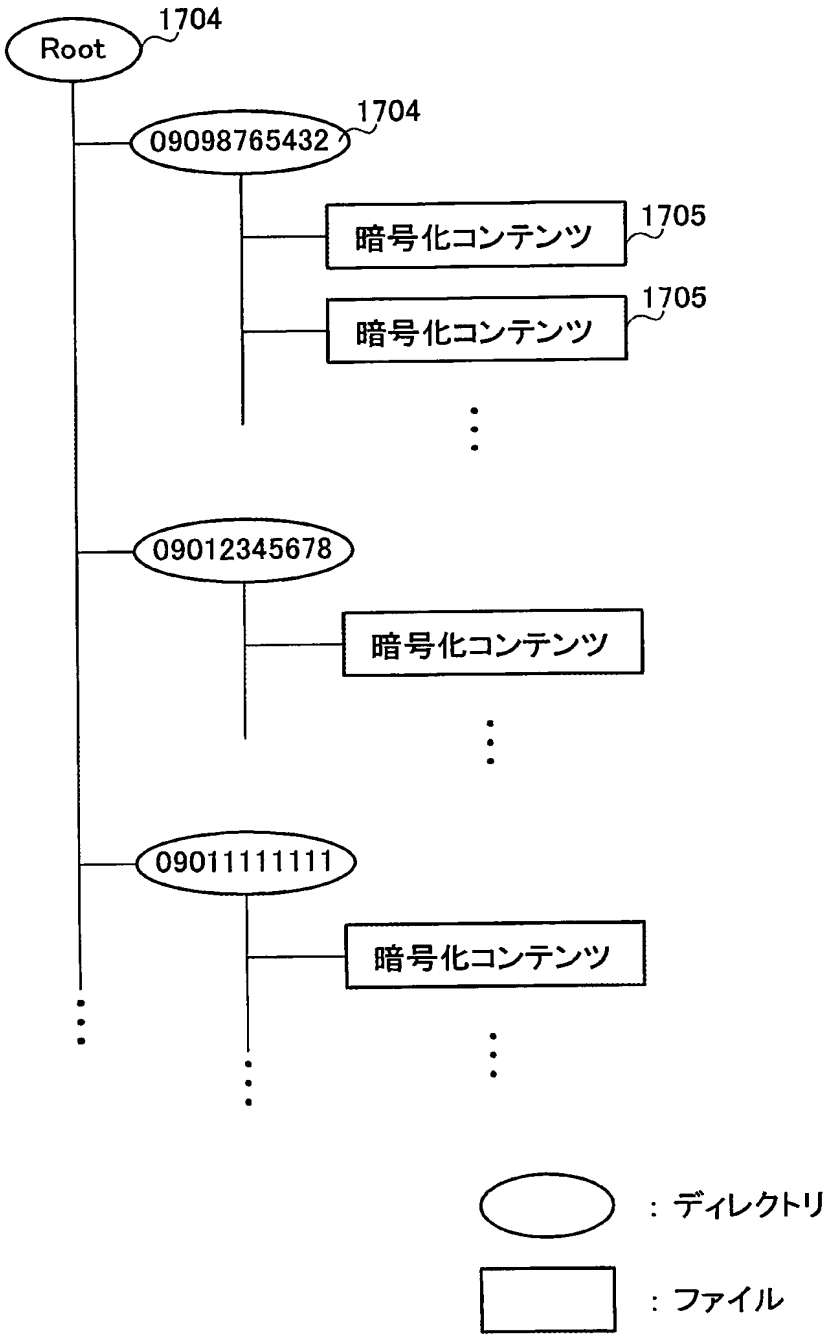

Root
1704
09098765432
1704
暗号化コンテンツ
1705
暗号化コンテンツ
1705
09012345678
暗号化コンテンツ
09011111111
暗号化コンテンツ
：ディレクトリ
：ファイル

図 20

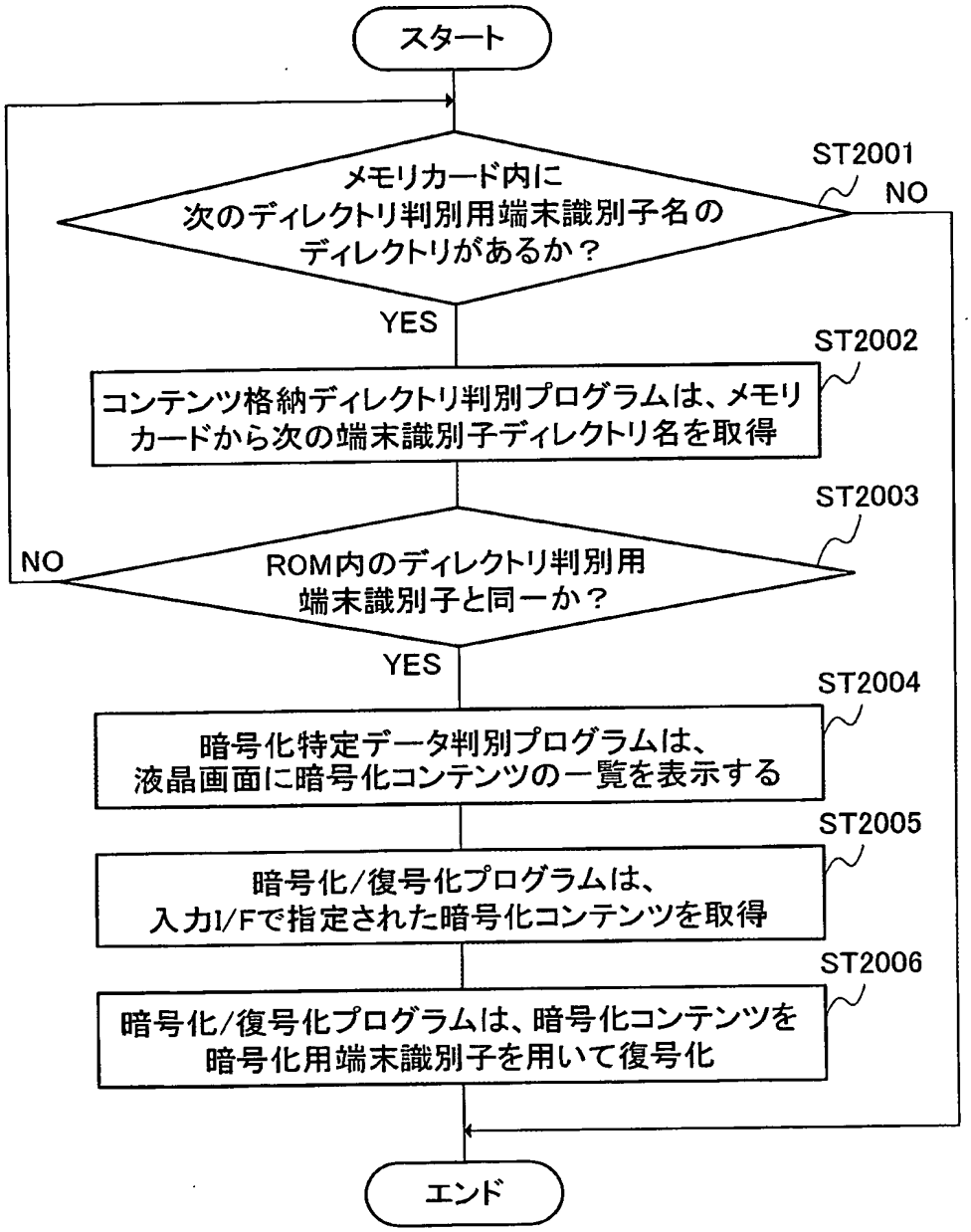

スタート
メモリカード内に
次のディレクトリ判別用端末識別子名の
ディレクトリがあるか？
ST2001
NO
YES
ST2002
コンテンツ格納ディレクトリ判別プログラムは、メモリ
カードから次の端末識別子ディレクトリ名を取得
ST2003
NO
ROM内のディレクトリ判別用
端末識別子と同一か？
YES
ST2004
暗号化特定データ判別プログラムは、
液晶画面に暗号化コンテンツの一覧を表示する
ST2005
暗号化/復号化プログラムは、
入力I/Fで指定された暗号化コンテンツを取得
ST2006
暗号化/復号化プログラムは、暗号化コンテンツを
暗号化用端末識別子を用いて復号化
エンド

図 21

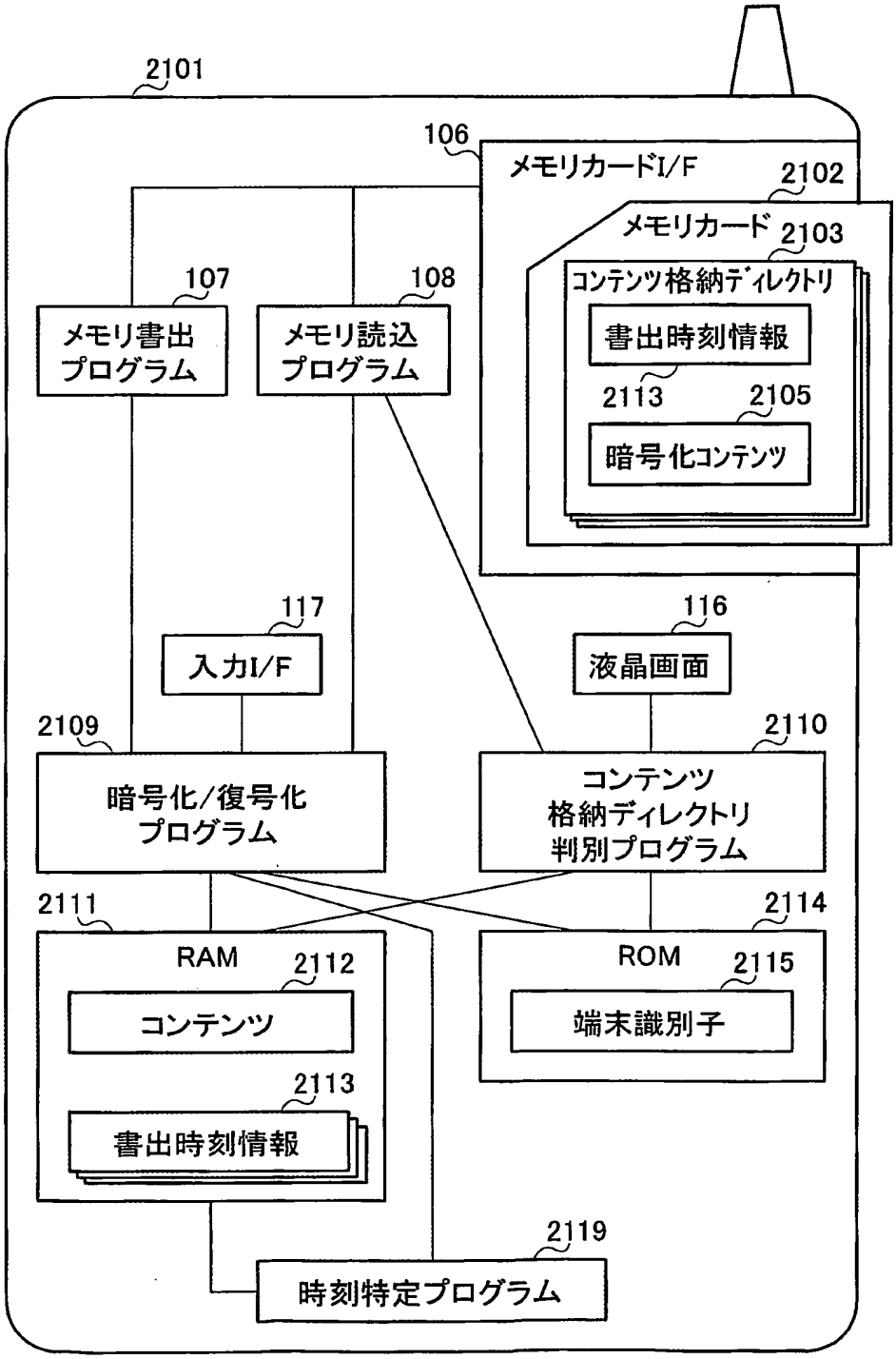

2101
106
メモリカードI/F
2102
メモリカード
2103
コンテンツ格納ディレクトリ
書出時刻情報
2113
2105
暗号化コンテンツ
107
メモリ書出
プログラム
108
メモリ読込
プログラム
117
入力I/F
116
液晶画面
2109
暗号化/復号化
プログラム
2110
コンテンツ
格納ディレクトリ
判別プログラム
2111
RAM
2112
コンテンツ
2113
書出時刻情報
2114
ROM
2115
端末識別子
2119
時刻特定プログラム

図 22

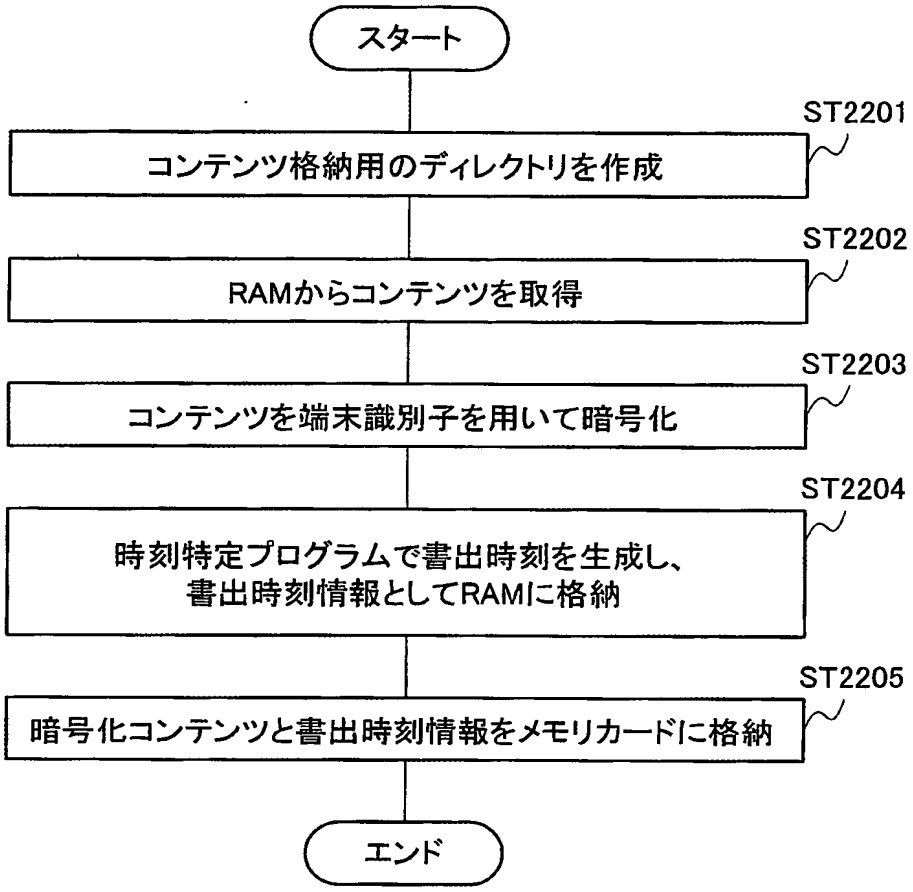

スタート
ST2201
コンテンツ格納用のディレクトリを作成
ST2202
RAMからコンテンツを取得
ST2203
コンテンツを端末識別子を用いて暗号化
ST2204
時刻特定プログラムで書出時刻を生成し、
書出時刻情報としてRAMに格納
ST2205
暗号化コンテンツと書出時刻情報をメモリカードに格納
エンド

図 23

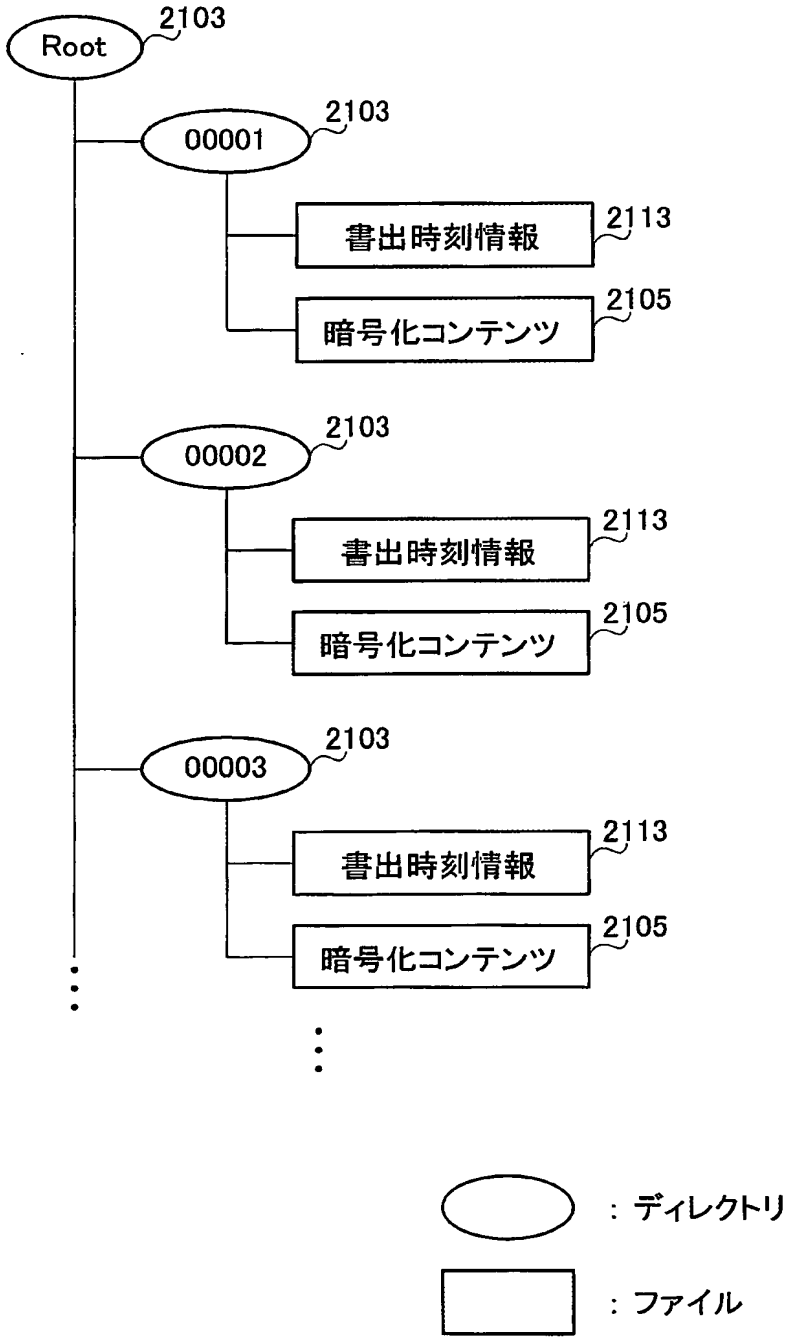

Root
2103
00001
2103
書出時刻情報
2113
暗号化コンテンツ
2105
00002
2103
書出時刻情報
2113
暗号化コンテンツ
2105
00003
2103
書出時刻情報
2113
暗号化コンテンツ
2105
：ディレクトリ
：ファイル

図 24

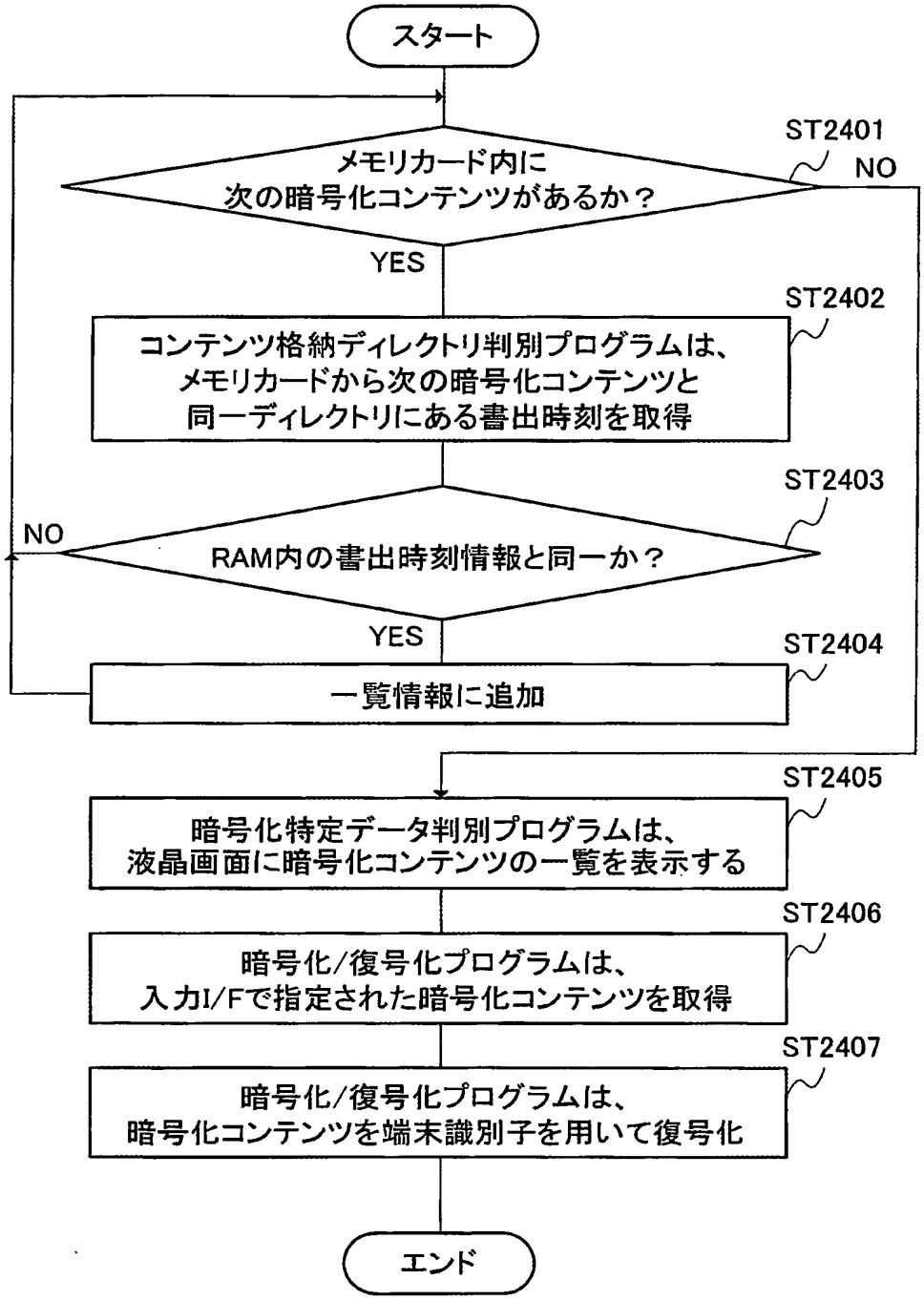

スタート
ST2401
メモリカード内に
次の暗号化コンテンツがあるか？
NO
YES
ST2402
コンテンツ格納ディレクトリ判別プログラムは、
メモリカードから次の暗号化コンテンツと
同一ディレクトリにある書出時刻を取得
ST2403
NO
RAM内の書出時刻情報と同一か？
YES
ST2404
一覧情報に追加
ST2405
暗号化特定データ判別プログラムは、
液晶画面に暗号化コンテンツの一覧を表示する
ST2406
暗号化/復号化プログラムは、
入力I/Fで指定された暗号化コンテンツを取得
ST2407
暗号化/復号化プログラムは、
暗号化コンテンツを端末識別子を用いて復号化
エンド

図 25

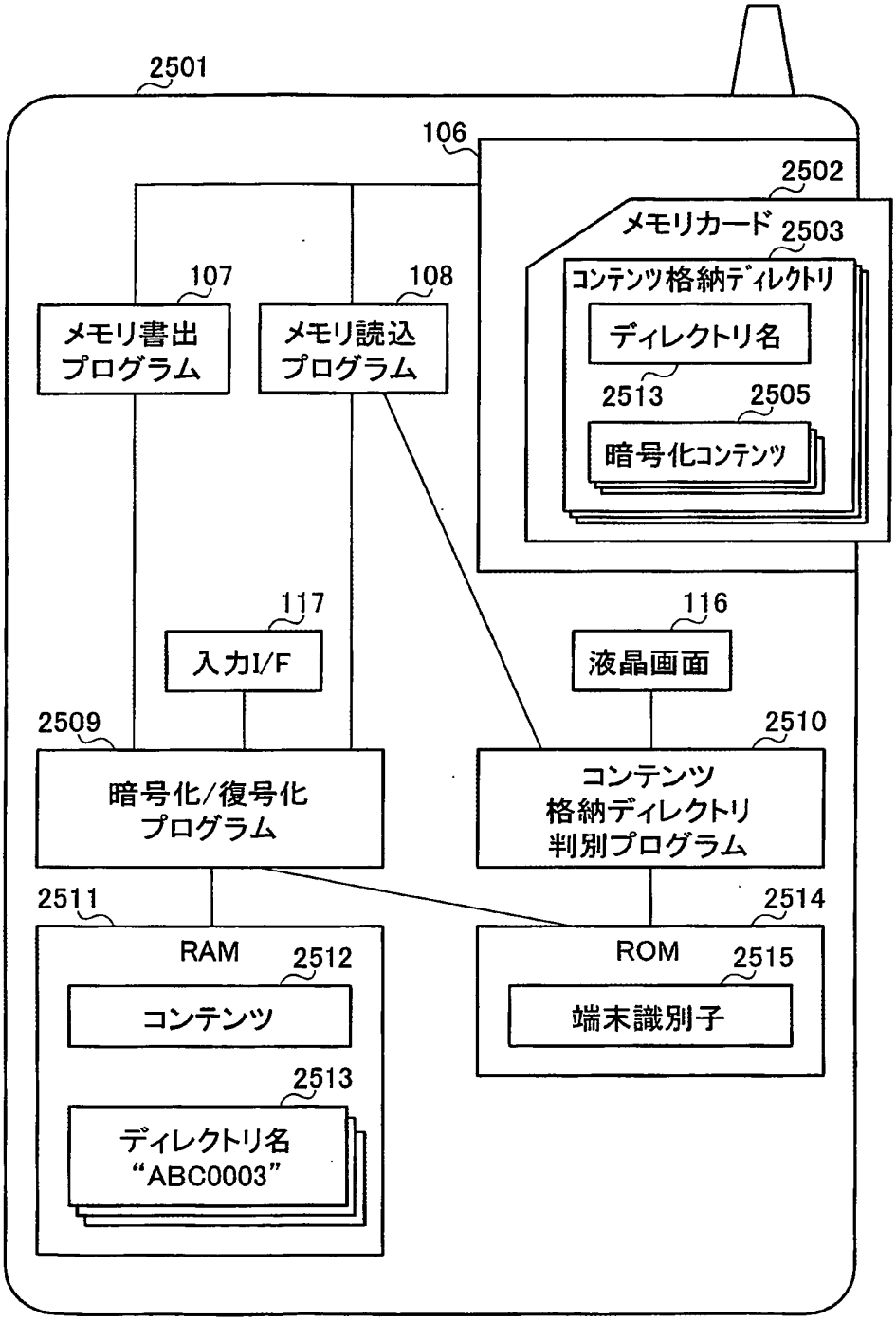

2501
106
2502
メモリカード
2503
コンテンツ格納ディレクトリ
ディレクトリ名
2513
2505
暗号化コンテンツ
107
メモリ書出
プログラム
108
メモリ読込
プログラム
117
入力I/F
116
液晶画面
2509
暗号化/復号化
プログラム
2510
コンテンツ
格納ディレクトリ
判別プログラム
2511
RAM
2512
コンテンツ
2513
ディレクトリ名
“ABC0003”
2514
ROM
2515
端末識別子

図 26

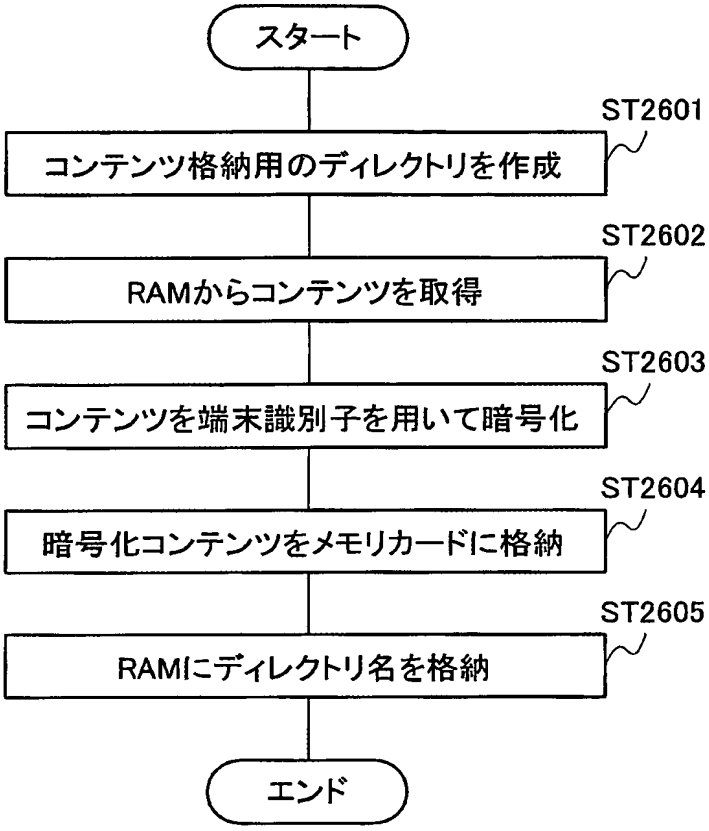

スタート
ST2601
コンテンツ格納用のディレクトリを作成
ST2602
RAMからコンテンツを取得
ST2603
コンテンツを端末識別子を用いて暗号化
ST2604
暗号化コンテンツをメモリカードに格納
ST2605
RAMにディレクトリ名を格納
エンド

図 27

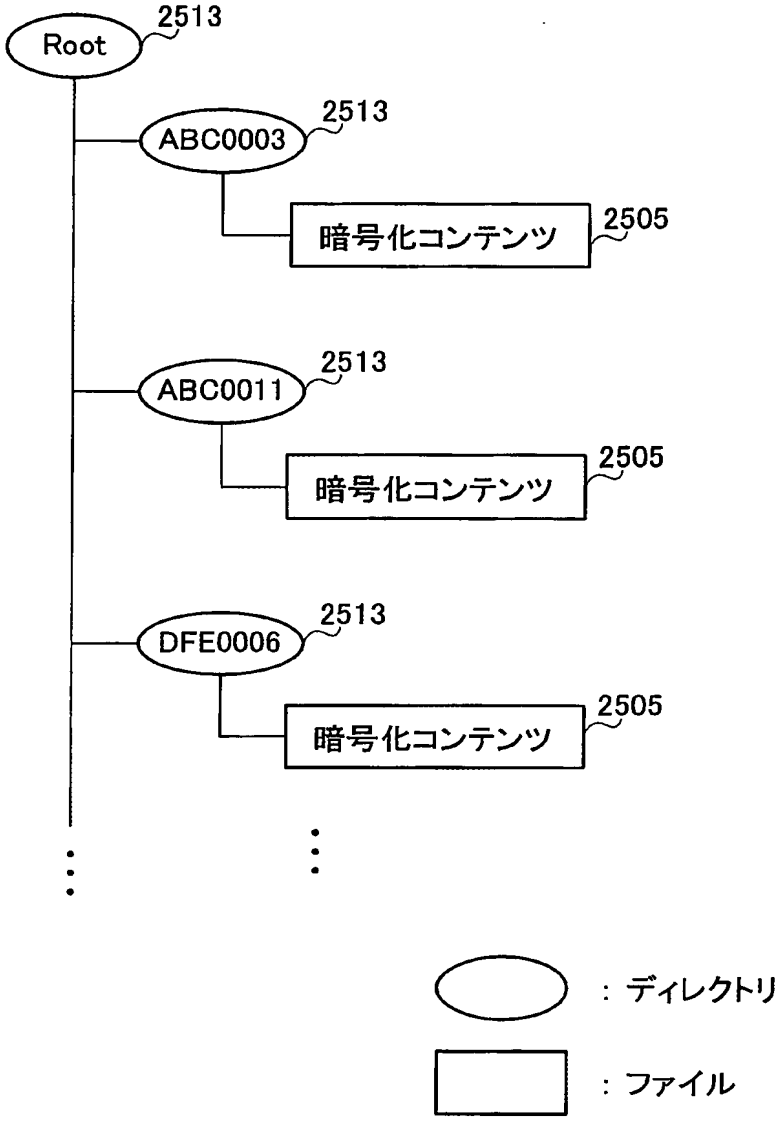

Root
2513
ABC0003
2513
暗号化コンテンツ
2505
ABC0011
2513
暗号化コンテンツ
2505
DFE0006
2513
暗号化コンテンツ
2505
：ディレクトリ
：ファイル

図 28

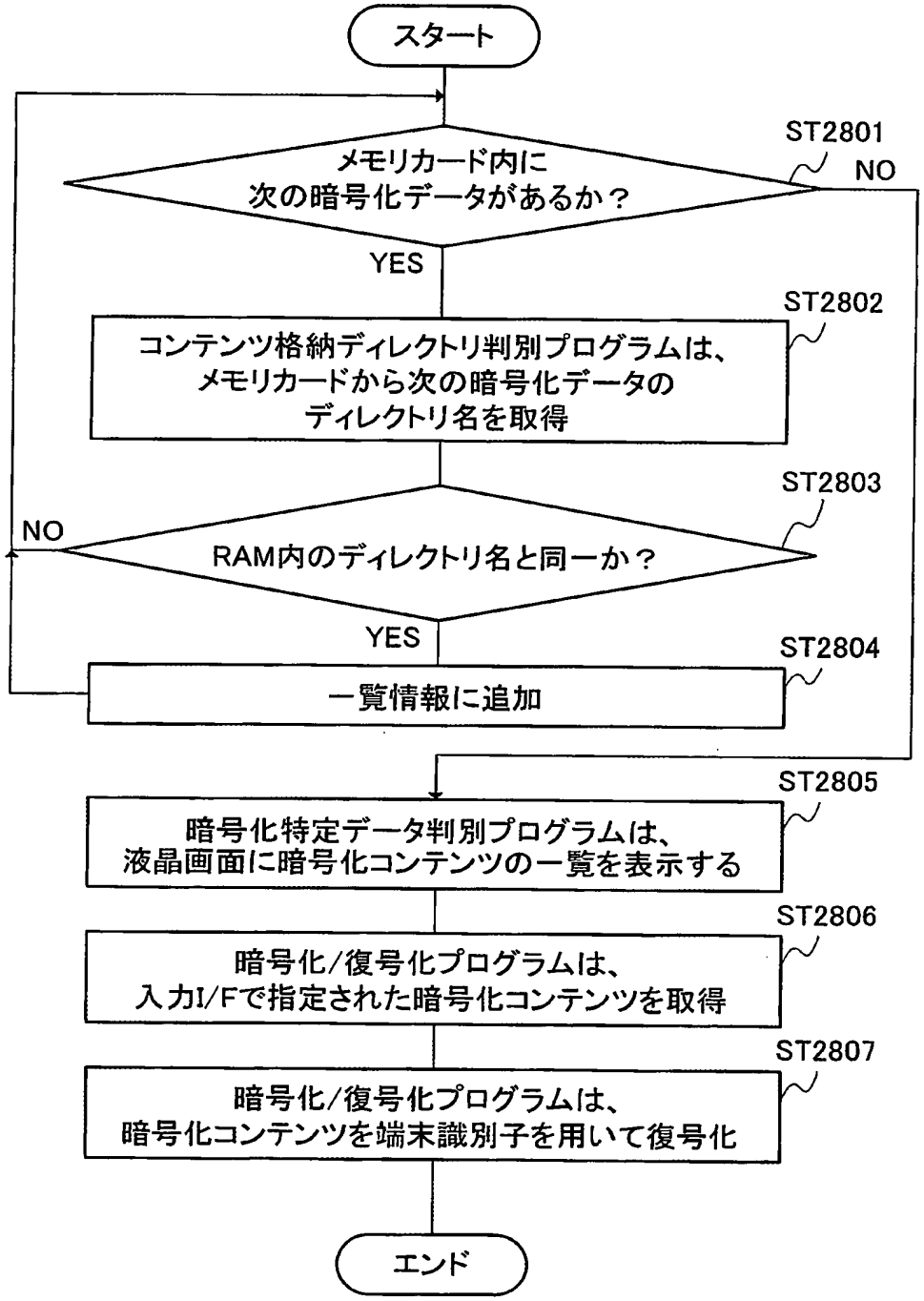

スタート
ST2801
メモリカード内に
次の暗号化データがあるか？
NO
YES
ST2802
コンテンツ格納ディレクトリ判別プログラムは、
メモリカードから次の暗号化データの
ディレクトリ名を取得
ST2803
NO
RAM内のディレクトリ名と同一か？
YES
ST2804
一覧情報に追加
ST2805
暗号化特定データ判別プログラムは、
液晶画面に暗号化コンテンツの一覧を表示する
ST2806
暗号化/復号化プログラムは、
入力I/Fで指定された暗号化コンテンツを取得
ST2807
暗号化/復号化プログラムは、
暗号化コンテンツを端末識別子を用いて復号化
エンド

図 29

国際調査報告

国際出願番号 PCT／JP03／02291

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl' H04L9／08 G11B20／10 G06F12／14 H04M11／00

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl' H04L9／08 G11B20／10 G06F12／14 H04M11／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2003年
日本国登録実用新案公報	1994－2003年
日本国実用新案登録公報	1996－2003年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2002－9966 A（ソフト流通株式会社） 2002.01.11，全文，図1－5 （ファミリーなし）	1－46
Y	JP 4－347949 A（株式会社東芝） 1992.12.03，第【0048】－【0050】段落 & DE 69128981 C & EP 460538 A & US 5136642 A & EP 735723 A	1－46

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 12.05.03	国際調査報告の発送日 27.05.03
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 青木 重徳　5M　4229 電話番号 03－3581－1101 内線 3597

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０３／０２２９１

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ　９－３０７５４３　Ａ（松下電器産業株式会社） １９９７．１１．２８，全文，図１－８ （ファミリーなし）	１－４６